

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001398

International filing date: 01 February 2005 (01.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-026850
Filing date: 03 February 2004 (03.02.2004)

Date of receipt at the International Bureau: 31 March 2005 (31.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

04. 2. 2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2004年 2月 3日
Date of Application:

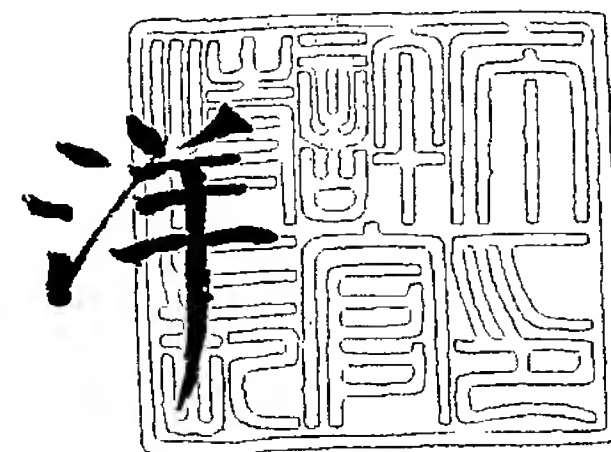
出願番号 特願2004-026850
Application Number:
[ST. 10/C]: [JP 2004-026850]

出願人 松下電器産業株式会社
Applicant(s):

2005年 3月17日

特許庁長官
Commissioner,
Japan Patent Office

小川



【書類名】 特許願
【整理番号】 2048160029
【提出日】 平成16年 2月 3日
【あて先】 特許庁長官 殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 横田 薫
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 原田 俊治
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 井藤 好克
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 藤村 一哉
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】 特許請求の範囲**【請求項 1】**

コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、

前記端末装置は、第 1 の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、

前記第 1 の暗号化されたコンテンツを前記可搬媒体に移動する際、前記第 1 の鍵記憶部に記憶する鍵を消去して、前記第 1 の暗号化されたコンテンツを利用不可状態にして、

前記可搬媒体は、第 2 の暗号化されたコンテンツを記録するコンテンツ記録領域を備え

、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする著作権保護システム。

【請求項 2】

前記著作権保護システムであって、

前記端末装置は、前記第 1 の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化するための鍵を記憶する第 2 の鍵記憶部と、前記可搬媒体に記録するコンテンツを暗号化する第 1 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第 1 の暗号化されたコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で復号して、前記第 1 の暗号化部において、前記復号したコンテンツを、前記第 2 の鍵記憶部に記憶する鍵で暗号化して、前記第 2 の暗号化されたコンテンツを生成することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 3】

前記著作権保護システムであって、

前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 1 の鍵記憶部に記憶する鍵を移動させ、その後、前記第 2 の鍵記憶部に記憶する鍵を移動させることを特徴とする請求項 2 記載の著作権保護システム。

【請求項 4】

前記著作権保護システムであって、

前記端末装置は、復号されたコンテンツに鍵を埋め込む埋込部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記埋込部において、前記第 1 の鍵記憶部に記憶する鍵を、前記移動するコンテンツに埋め込むことを特徴とする請求項 2 記載の著作権保護システム。

【請求項 5】

前記著作権保護システムであって、

前記端末装置は、前記端末装置固有の鍵を記憶する第 3 の鍵記憶部と、前記第 1 の鍵記憶部に記憶する鍵を暗号化する第 2 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 2 の暗号化部において、前記第 1 の鍵記憶部に記憶する鍵を、前記第 3 の鍵記憶部に記憶する鍵で暗号化することを特徴とする請求項 2 記載の著作権保護システム。

【請求項 6】

前記著作権保護システムであって、

前記端末装置は、前記第 1 の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化する第 1 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第 1 の暗号化されたコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で復号して、前記第 1 の暗号化部において、前記復号したコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で暗号化して、前記第 2 の暗号化されたコンテンツを生成することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 7】

前記著作権保護システムであって、

前記端末装置は、前記端末装置固有の鍵を記憶する第 3 の鍵記憶部と、前記第 1 の鍵記憶部に記憶する鍵を暗号化する第 2 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 2 の暗号化部において、前記第 1 の鍵記憶部に記憶する鍵を、前記第 3 の鍵記憶部に記憶する鍵で暗号化することを特徴とする請求項 6 記載の著作権保護システム。

【請求項 8】

前記著作権保護システムであって、

前記端末装置は、前記コンテンツの移動状態を保持する状態保持部を備え、

前記端末装置は、前記コンテンツの移動が正しく完了しなかった場合、前記状態保持部が保持する状態に基づいて再動作を行うことを特徴とする請求項 1 記載の著作権保護システム。

【請求項 9】

前記著作権保護システムであって、

前記端末装置は、前記コンテンツの移動状態を利用者に通知する通知部を備え、

前記通知部は、前記状態保持部に保持されるコンテンツの移動状態を利用者に通知することを特徴とする請求項 8 記載の著作権保護システム。

【請求項 10】

コンテンツを保持して、可搬媒体へコンテンツを移動可能な端末装置であって、

前記端末装置は、第 1 の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、

前記第 1 の暗号化されたコンテンツを前記可搬媒体に移動する際、前記第 1 の鍵記憶部に記憶する鍵を消去して、前記第 1 の暗号化されたコンテンツを利用不可状態にすることを特徴とする端末装置。

【請求項 11】

前記端末装置であって、

前記端末装置は、前記第 1 の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化するための鍵を記憶する第 2 の鍵記憶部と、前記可搬媒体に記録するコンテンツを暗号化する第 1 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第 1 の暗号化されたコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で復号して、前記第 1 の暗号化部において、前記復号したコンテンツを、前記第 2 の鍵記憶部に記憶する鍵で暗号化して、前記第 2 の暗号化されたコンテンツを生成することを特徴とする請求項 10 記載の端末装置。

【請求項 12】

前記端末装置であって、

前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 1 の鍵記憶部に記憶する鍵を移動させ、その後、前記第 2 の鍵記憶部に記憶する鍵を移動させることを特徴とする請求項 11 記載の端末装置。

【請求項 13】

前記端末装置であって、

前記端末装置は、復号されたコンテンツに鍵を埋め込む埋込部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記埋込部において、前記第 1 の鍵記憶部に記憶する鍵を、前記移動するコンテンツに埋め込むことを特徴とする請求項 11 記載の端末装置。

【請求項 14】

前記端末装置であって、

前記端末装置は、前記端末装置固有の鍵を記憶する第 3 の鍵記憶部と、前記第 1 の鍵記憶部に記憶する鍵を暗号化する第 2 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 2 の暗号化部にお

いて、前記第 1 の鍵記憶部に記憶する鍵を、前記第 3 の鍵記憶部に記憶する鍵で暗号化することを特徴とする請求項 1 1 記載の端末装置。

【請求項 1 5】

前記端末装置であって、

前記端末装置は、前記第 1 の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化する第 1 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第 1 の暗号化されたコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で復号して、前記第 1 の暗号化部において、前記復号したコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で暗号化して、前記第 2 の暗号化されたコンテンツを生成することを特徴とする請求項 1 0 記載の端末装置。

【請求項 1 6】

前記端末装置であって、

前記端末装置は、前記端末装置固有の鍵を記憶する第 3 の鍵記憶部と、前記第 1 の鍵記憶部に記憶する鍵を暗号化する第 2 の暗号化部を備え、

前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 2 の暗号化部において、前記第 1 の鍵記憶部に記憶する鍵を、前記第 3 の鍵記憶部に記憶する鍵で暗号化することを特徴とする請求項 1 5 記載の端末装置。

【請求項 1 7】

前記端末装置であって、

前記端末装置は、前記コンテンツの移動状態を保持する状態保持部を備え、

前記端末装置は、前記コンテンツの移動が正しく完了しなかった場合、前記状態保持部が保持する状態に基づいて再動作を行うことを特徴とする請求項 1 0 記載の端末装置。

【請求項 1 8】

前記端末装置であって、

前記端末装置は、前記コンテンツの移動状態を利用者に通知する通知部を備え、

前記通知部は、前記状態保持部に保持されるコンテンツの移動状態を利用者に通知することを特徴とする請求項 1 7 記載の端末装置。

【請求項 1 9】

利用不可状態のコンテンツを保持する端末装置が、可搬媒体から前記コンテンツを利用可能状態にするために必要なデータを読み出し、前記端末装置のコンテンツを利用可能状態にする著作権保護システムであって、

前記端末装置は、第 1 の暗号化されたコンテンツを記憶する第 1 の記憶部と、前記第 1 のコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、

前記可搬媒体は、前記第 1 の暗号化されたコンテンツを復号するために必要なデータを記録するデータ記録領域を備え、

前記端末装置は、前記可搬媒体から前記データ記録領域に記録するデータを受信して、前記受信したデータに基づいて、前記第 1 の記憶部に記憶する暗号化コンテンツを復号するために必要な鍵を獲得して、前記第 1 の鍵記憶部に前記鍵を記憶することを特徴とする著作権保護システム。

【請求項 2 0】

前記著作権保護システムであって、

前記端末装置は、前記端末装置固有の鍵を記憶する第 2 の鍵記憶部を備え、

前記可搬媒体の前記データ記録領域に記録するデータは、前記第 1 の記憶部に記憶する鍵を、前記第 2 の鍵記憶部に記憶する鍵を用いて暗号化したデータであることを特徴とする請求項 1 9 記載の著作権保護システム。

【請求項 2 1】

前記著作権保護システムであって、

前記端末装置は、コンテンツに埋め込まれた鍵を抽出する抽出部を備え、

前記可搬媒体の前記データ記録領域に記録するデータは、第 2 の暗号化されたコンテ

ッ、並びに前記第 2 の暗号化されたコンテンツを復号するための鍵であり、さらに、前記第 2 の暗号化されたコンテンツには、前記第 1 のコンテンツを復号するための鍵が埋め込まれていることを特徴とする請求項 1 9 記載の著作権保護システム。

【請求項 2 2】

前記著作権保護システムであって、
前記可搬媒体の前記データ記録領域に記録するデータは、前記第 1 の暗号化されたコンテンツを復号するための鍵であることを特徴とする請求項 1 9 記載の著作権保護システム。

【請求項 2 3】

前記著作権保護システムであって、
前記コンテンツには、前記コンテンツを一意に識別するため識別子が付与されており、
前記端末装置は、前記可搬媒体から移動させるコンテンツと、前記記憶部に記憶するコンテンツの識別子が一致するか否かを判定する判定部を備え、
前記端末装置は、前記判定部で一致すると判定した場合に限りコンテンツの移動を実行することを特徴とする請求項 1 9 記載の著作権保護システム。

【請求項 2 4】

利用不可状態のコンテンツを保持して、可搬媒体から前記コンテンツを利用可能状態にするために必要なデータを読み出し、コンテンツを利用可能状態にする端末装置であって、

前記端末装置は、第 1 の暗号化されたコンテンツを記憶する第 1 の記憶部と、前記第 1 のコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、

前記可搬媒体は、前記第 1 の暗号化されたコンテンツを復号するために必要なデータを記録するデータ記録領域を備え、

前記端末装置は、前記可搬媒体から前記データ記録領域に記録するデータを受信して、前記受信したデータに基づいて、前記第 1 の記憶部に記憶する暗号化コンテンツを復号するために必要な鍵を獲得して、前記第 1 の鍵記憶部に前記鍵を記憶することを特徴とする端末装置。

【請求項 2 5】

前記端末装置であって、

前記端末装置は、前記端末装置固有の鍵を記憶する第 2 の鍵記憶部を備え、

前記可搬媒体の前記データ記録領域に記録するデータは、前記第 1 の記憶部に記憶する鍵を、前記第 2 の鍵記憶部に記憶する鍵を用いて暗号化したデータであることを特徴とする請求項 2 4 記載の端末装置。

【請求項 2 6】

前記端末装置であって、

前記端末装置は、コンテンツに埋め込まれた鍵を抽出する抽出部を備え、

前記可搬媒体の前記データ記録領域に記録するデータは、第 2 の暗号化されたコンテンツ、並びに前記第 2 の暗号化されたコンテンツを復号するための鍵であり、さらに、前記第 2 の暗号化されたコンテンツには、前記第 1 のコンテンツを復号するための鍵が埋め込まれていることを特徴とする請求項 2 4 記載の端末装置。

【請求項 2 7】

コンテンツを保持する第 1 の端末装置から、第 2 の端末装置へコンテンツを移動可能な著作権保護システムであって、

前記第 1 の端末装置は、第 1 の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、

前記第 1 の暗号化されたコンテンツを前記第 2 の端末装置に移動する際、前記第 1 の鍵記憶部に記憶する鍵を消去して、前記第 1 の暗号化されたコンテンツを利用不可状態にして、

前記第 2 の端末装置は、第 2 の暗号化されたコンテンツを記憶する記憶部を備え、

前記移動するコンテンツを前記記憶部に記憶することを特徴とする著作権保護システム

。

【請求項 2 8】

前記著作権保護システムであって、

前記第 2 の端末装置は、前記移動されるコンテンツの受信が完了したか否かを確認する確認部と、前記確認結果を通知する通知部を備え、

前記第 1 の端末装置は、前記第 2 の端末装置が通知する確認結果を受信した後、前記第 1 の鍵記憶部に記憶する鍵を消去することを特徴とする請求項 2 7 記載の著作権保護システム。

【請求項 2 9】

利用不可状態のコンテンツを保持する第 1 の端末装置が、第 2 の端末装置から前記コンテンツを利用可能状態にするために必要なデータを読み出し、前記第 1 の端末装置のコンテンツを利用可能状態にする著作権保護システムであって、

前記第 1 の端末装置は、第 1 の暗号化されたコンテンツを記憶する第 1 の記憶部と、前記第 1 のコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、

前記第 2 の端末装置は、前記第 1 の暗号化されたコンテンツを復号するために必要なデータを記憶するデータ記憶部を備え、

前記第 1 の端末装置は、前記第 2 の端末装置から前記データ記憶部に記憶するデータを受信して、前記受信したデータに基づいて、前記第 1 の記憶部に記憶する暗号化コンテンツを復号するために必要な鍵を獲得して、前記第 1 の鍵記憶部に前記鍵を記憶することを特徴とする著作権保護システム。

【請求項 3 0】

前記著作権保護システムであって、

前記第 1 の端末装置は、前記端末装置固有の鍵を記憶する第 2 の鍵記憶部を備え、

前記第 2 の端末装置の前記データ記憶部に記憶するデータは、前記第 1 の記憶部に記憶する鍵を、前記第 2 の鍵記憶部に記憶する鍵を用いて暗号化したデータであることを特徴とする請求項 2 9 記載の著作権保護システム。

【請求項 3 1】

前記著作権保護システムであって、

前記第 1 の端末装置は、コンテンツに埋め込まれた鍵を抽出する抽出部を備え、

前記第 2 の端末装置の前記データ記憶部に記憶するデータは、第 2 の暗号化されたコンテンツ、並びに前記第 2 の暗号化されたコンテンツを復号するための鍵であり、さらに、前記第 2 の暗号化されたコンテンツには、前記第 1 のコンテンツを復号するための鍵が埋め込まれていることを特徴とする請求項 2 9 記載の著作権保護システム。

【請求項 3 2】

前記著作権保護システムであって、

前記第 2 の端末装置の前記データ記憶部に記憶するデータは、前記第 1 の暗号化されたコンテンツを復号するための鍵であることを特徴とする請求項 2 9 記載の著作権保護システム。

【書類名】 明細書

【発明の名称】 記録再生装置及び著作権保護システム

【技術分野】

【0 0 0 1】

本発明は、コンテンツの不正利用防止を目的とした記録再生装置、及び可搬媒体を含む著作権保護システムに関し、特に、不正利用を防止しつつユーザの利便性を高める技術に関する。

【背景技術】

【0 0 0 2】

近年、BSデジタル放送や地上デジタル放送の開始に伴い、映画等のデジタルコンテンツが広く配信されるようになってきている。デジタルコンテンツ（以下、コンテンツ）は複製が容易であるため、インターネットやその他の媒体を介した海賊行為、並びに複製コンテンツの再配信などの不正行為に対する懸念が高まっており、これら不正行為に対抗（コンテンツを保護）するための技術開発が進められている。

【0 0 0 3】

このようなコンテンツの保護技術に関する規格として、例えば、DTCP (Digital Transmission Content Protection) がある。DTCPは、コンテンツをデジタル転送する際に、コンテンツを暗号化するなどして不正コピーを防止する技術である。DTCPのようなコンテンツ保護技術においては、コンテンツに、「Copy No More」、「Copy One Generation」等のコピー制御情報 (CCI: Copy Control Information) を付与する。「Copy No More」はコンテンツのコピーが禁止されていることを表し、「Copy One Generation」はコンテンツのコピーが1回だけ許されていることを表す。従って、コピー制御情報として「Copy One Generation」が付与されたコンテンツをコピーすると、コピーによって新たに得られたコンテンツには、コピー制御情報として「Copy No More」が付与される。

【0 0 0 4】

一方で、コピー制御情報として「Copy No More」が付与されたコンテンツであっても、他の記録媒体、あるいは他の装置へ移動させたいという要望がある。例えば、デジタルテレビに内蔵されているHDD (Hard Disk Drive) に記録されているコンテンツをDVD-RAMに移動させて保存版として保管しておきたいような場合である。この際 (HDDからDVD-RAMにコンテンツを移動させた場合)、デジタルテレビ内蔵HDDの当該コンテンツは、当然、再生できない状態にされなければならない。例えば、内蔵HDDからDVD-RAMにコンテンツをコピーした後に、内蔵HDDに記録されているコンテンツを消去するなどしてコンテンツを無効化する、すなわちコンテンツを利用できない状態にする方法などが考えられる。しかしながら、コンテンツの移動に先立ってデジタルテレビから内蔵HDDを取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、コンテンツを移動した後にバックアップしておいたデータを内蔵HDDに戻すという操作が行われると、コンテンツを何度でも移動できることになり、事実上不正コピーを防止することができなくなる。

【0 0 0 5】

また、コンテンツの移動中に電源断などの原因により、移動元と移動先のコンテンツが共に損なわれ、コンテンツとして利用できなくなることは、コンテンツを利用するユーザにとっては不便である。さらに、このようにして利用できなくなったコンテンツを再度入手するために出費が必要な場合には経済的な損失も発生する。

上記課題を解決するための従来技術として、不正コピーを防止しながら、コンテンツの喪失を招くことなく、コンテンツの移動を可能にする技術が特許文献1に開示されている。

【特許文献1】 特開 2 0 0 3 - 2 2 8 5 2 2 号公報

【非特許文献1】 「現代暗号理論」、池野信一、小山謙二、電子通信学会

出証特 2 0 0 5 - 3 0 2 3 6 9 2

【非特許文献2】「暗号理論入門」、岡本栄司、共立出版株式会社

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、移動元のコンテンツが高画質コンテンツであり、コンテンツのサイズに比べて、移動先の記録容量が小さい場合には、コンテンツの移動前に、その画質を劣化させるなどしてサイズを小さく圧縮変換してから移動を行うのが通例であるが、前記構成のようにコンテンツを消去するなどして移動元のコンテンツを無効化する場合、圧縮変換された（画質の劣化した）コンテンツだけがユーザの下に残ることになる。すなわち、再び記録容量の大きな内蔵HDDへコンテンツを戻す（移動する）場合であっても、画質の劣化されたコンテンツを高画質コンテンツへ変換することは不可能であり、元々の高画質コンテンツは復元されないため、これはコンテンツを利用するユーザの利便性が損なわれることにつながる。

【0007】

本発明は、前記課題を解決するものであって、不正コピーを防止しながら、コンテンツの喪失を招くことなくコンテンツの移動を可能にして、さらに、サイズを小さくする圧縮変換後であっても、当該コンテンツを移動元に戻す場合には、元々の高画質コンテンツの復元を可能にする記録再生装置、並びに可搬媒体を含む著作権保護システムの提供を目的とする。

【課題を解決するための手段】

【0008】

本発明は、コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、前記端末装置は、第1の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第1の鍵記憶部を備え、前記第1の暗号化されたコンテンツを前記可搬媒体に移動する際、前記第1の鍵記憶部に記憶する鍵を消去して、前記第1の暗号化されたコンテンツを利用不可状態にして、前記可搬媒体は、第2の暗号化されたコンテンツを記録するコンテンツ記録領域を備え、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とするコンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、前記端末装置は、第1の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第1の鍵記憶部を備え、前記第1の暗号化されたコンテンツを前記可搬媒体に移動する際、前記第1の鍵記憶部に記憶する鍵を消去して、前記第1の暗号化されたコンテンツを利用不可状態にして、前記可搬媒体は、第2の暗号化されたコンテンツを記録するコンテンツ記録領域を備え、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする。

【0009】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記第1の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化するための鍵を記憶する第2の鍵記憶部と、前記可搬媒体に記録するコンテンツを暗号化する第1の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第1の暗号化されたコンテンツを、前記第1の鍵記憶部に記憶する鍵で復号して、前記第1の暗号化部において、前記復号したコンテンツを、前記第2の鍵記憶部に記憶する鍵で暗号化して、前記第2の暗号化されたコンテンツを生成することを特徴とする。

【0010】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第1の鍵記憶部に記憶する鍵を移動させ、その後、前記第2の鍵記憶部に記憶する鍵を移動させることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、復号されたコンテンツに鍵を埋め込む埋込部を備え、前記端末装置から前記可搬媒体へコンテンツを移動

する際に、前記埋込部において、前記第 1 の鍵記憶部に記憶する鍵を、前記移動するコンテンツに埋め込むことを特徴とする。

【0011】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記端末装置固有の鍵を記憶する第 3 の鍵記憶部と、前記第 1 の鍵記憶部に記憶する鍵を暗号化する第 2 の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 2 の暗号化部において、前記第 1 の鍵記憶部に記憶する鍵を、前記第 3 の鍵記憶部に記憶する鍵で暗号化することを特徴とする。

【0012】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記第 1 の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化する第 1 の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第 1 の暗号化されたコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で復号して、前記第 1 の暗号化部において、前記復号したコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で暗号化して、前記第 2 の暗号化されたコンテンツを生成することを特徴とする。

【0013】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記端末装置固有の鍵を記憶する第 3 の鍵記憶部と、前記第 1 の鍵記憶部に記憶する鍵を暗号化する第 2 の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 2 の暗号化部において、前記第 1 の鍵記憶部に記憶する鍵を、前記第 3 の鍵記憶部に記憶する鍵で暗号化することを特徴とする。

【0014】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記コンテンツの移動状態を保持する状態保持部を備え、前記端末装置は、前記コンテンツの移動が正しく完了しなかった場合、前記状態保持部が保持する状態に基づいて再動作を行うことを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記コンテンツの移動状態を利用者に通知する通知部を備え、前記通知部は、前記状態保持部に保持されるコンテンツの移動状態を利用者に通知することを特徴とする。

【0015】

また、本発明は、コンテンツを保持して、可搬媒体へコンテンツを移動可能な端末装置であって、前記端末装置は、第 1 の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、前記第 1 の暗号化されたコンテンツを前記可搬媒体に移動する際、前記第 1 の鍵記憶部に記憶する鍵を消去して、前記第 1 の暗号化されたコンテンツを利用不可状態にすることを特徴とする。

【0016】

また、本発明は、前記端末装置であって、前記端末装置は、前記第 1 の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化するための鍵を記憶する第 2 の鍵記憶部と、前記可搬媒体に記録するコンテンツを暗号化する第 1 の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第 1 の暗号化されたコンテンツを、前記第 1 の鍵記憶部に記憶する鍵で復号して、前記第 1 の暗号化部において、前記復号したコンテンツを、前記第 2 の鍵記憶部に記憶する鍵で暗号化して、前記第 2 の暗号化されたコンテンツを生成することを特徴とする。

【0017】

また、本発明は、前記端末装置であって、前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 1 の鍵記憶部に記憶する鍵を移動させ、その後、前記第 2 の鍵記憶部に記憶する鍵を移動させることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、復号されたコンテンツに鍵を埋め込む埋込部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記埋込部において、前記第1の鍵記憶部に記憶する鍵を、前記移動するコンテンツに埋め込むことを特徴とする。

【0018】

また、本発明は、前記端末装置であって、前記端末装置は、前記端末装置固有の鍵を記憶する第3の鍵記憶部と、前記第1の鍵記憶部に記憶する鍵を暗号化する第2の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第2の暗号化部において、前記第1の鍵記憶部に記憶する鍵を、前記第3の鍵記憶部に記憶する鍵で暗号化することを特徴とする。

【0019】

また、本発明は、前記端末装置であって、前記端末装置は、前記第1の暗号化されたコンテンツを復号する復号部と、前記可搬媒体に記録するコンテンツを暗号化する第1の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記復号部において、前記第1の暗号化されたコンテンツを、前記第1の鍵記憶部に記憶する鍵で復号して、前記第1の暗号化部において、前記復号したコンテンツを、前記第1の鍵記憶部に記憶する鍵で暗号化して、前記第2の暗号化されたコンテンツを生成することを特徴とする。

【0020】

また、本発明は、前記端末装置であって、前記端末装置は、前記端末装置固有の鍵を記憶する第3の鍵記憶部と、前記第1の鍵記憶部に記憶する鍵を暗号化する第2の暗号化部を備え、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第2の暗号化部において、前記第1の鍵記憶部に記憶する鍵を、前記第3の鍵記憶部に記憶する鍵で暗号化することを特徴とする。

【0021】

また、本発明は、前記端末装置であって、前記端末装置は、前記コンテンツの移動状態を保持する状態保持部を備え、前記端末装置は、前記コンテンツの移動が正しく完了しなかった場合、前記状態保持部が保持する状態に基づいて再動作を行うことを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記コンテンツの移動状態を利用者に通知する通知部を備え、前記通知部は、前記状態保持部に保持されるコンテンツの移動状態を利用者に通知することを特徴とする。

【0022】

また、本発明は、利用不可状態のコンテンツを保持する端末装置が、可搬媒体から前記コンテンツを利用可能状態にするために必要なデータを読み出し、前記端末装置のコンテンツを利用可能状態にする著作権保護システムであって、前記端末装置は、第1の暗号化されたコンテンツを記憶する第1の記憶部と、前記第1のコンテンツを復号するための鍵を記憶する第1の鍵記憶部を備え、前記可搬媒体は、前記第1の暗号化されたコンテンツを復号するために必要なデータを記録するデータ記録領域を備え、前記端末装置は、前記可搬媒体から前記データ記録領域に記録するデータを受信して、前記受信したデータに基づいて、前記第1の記憶部に記憶する暗号化コンテンツを復号するために必要な鍵を獲得して、前記第1の鍵記憶部に前記鍵を記憶することを特徴とする。

【0023】

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記端末装置固有の鍵を記憶する第2の鍵記憶部を備え、前記可搬媒体の前記データ記録領域に記録するデータは、前記第1の記憶部に記憶する鍵を、前記第2の鍵記憶部に記憶する鍵を用いて暗号化したデータであることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、コンテンツに埋め込まれた鍵を抽出する抽出部を備え、前記可搬媒体の前記データ記録領域に記録するデータは、第2の暗号化されたコンテンツ、並びに前記第2の暗号化されたコンテンツを復号するための鍵であり、さらに、前記第2の暗号化されたコンテンツには、前記第1の

ンテンツを復号するための鍵が埋め込まれていることを特徴とする。

【 0 0 2 4 】

また、本発明は、前記著作権保護システムであって、前記可搬媒体の前記データ記録領域に記録するデータは、前記第 1 の暗号化されたコンテンツを復号するための鍵であることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記コンテンツには、前記コンテンツを一意に識別するため識別子が付与されており、前記端末装置は、前記可搬媒体から移動させるコンテンツと、前記記憶部に記憶するコンテンツの識別子が一致するか否かを判定する判定部を備え、前記端末装置は、前記判定部で一致すると判定した場合に限りコンテンツの移動を実行することを特徴とする。

【 0 0 2 5 】

また、本発明は、利用不可状態のコンテンツを保持して、可搬媒体から前記コンテンツを利用可能状態にするために必要なデータを読み出し、コンテンツを利用可能状態にする端末装置であって、前記端末装置は、第 1 の暗号化されたコンテンツを記憶する第 1 の記憶部と、前記第 1 のコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、前記可搬媒体は、前記第 1 の暗号化されたコンテンツを復号するために必要なデータを記録するデータ記録領域を備え、前記端末装置は、前記可搬媒体から前記データ記録領域に記録するデータを受信して、前記受信したデータに基づいて、前記第 1 の記憶部に記憶する暗号化コンテンツを復号するために必要な鍵を獲得して、前記第 1 の鍵記憶部に前記鍵を記憶することを特徴とする。

【 0 0 2 6 】

また、本発明は、前記端末装置であって、前記端末装置は、前記端末装置固有の鍵を記憶する第 2 の鍵記憶部を備え、前記可搬媒体の前記データ記録領域に記録するデータは、前記第 1 の記憶部に記憶する鍵を、前記第 2 の鍵記憶部に記憶する鍵を用いて暗号化したデータであることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、コンテンツに埋め込まれた鍵を抽出する抽出部を備え、前記可搬媒体の前記データ記録領域に記録するデータは、第 2 の暗号化されたコンテンツ、並びに前記第 2 の暗号化されたコンテンツを復号するための鍵であり、さらに、前記第 2 の暗号化されたコンテンツには、前記第 1 のコンテンツを復号するための鍵が埋め込まれていることを特徴とする。

【 0 0 2 7 】

また、本発明は、コンテンツを保持する第 1 の端末装置から、第 2 の端末装置へコンテンツを移動可能な著作権保護システムであって、前記第 1 の端末装置は、第 1 の暗号化されたコンテンツを記憶する記憶部と、前記暗号化されたコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、前記第 1 の暗号化されたコンテンツを前記第 2 の端末装置に移動する際、前記第 1 の鍵記憶部に記憶する鍵を消去して、前記第 1 の暗号化されたコンテンツを利用不可状態にして、前記第 2 の端末装置は、第 2 の暗号化されたコンテンツを記憶する記憶部を備え、前記移動するコンテンツを前記記憶部に記憶することを特徴とする。

【 0 0 2 8 】

また、本発明は、前記著作権保護システムであって、前記第 2 の端末装置は、前記移動されるコンテンツの受信が完了したか否かを確認する確認部と、前記確認結果を通知する通知部を備え、前記第 1 の端末装置は、前記第 2 の端末装置が通知する確認結果を受信した後、前記第 1 の鍵記憶部に記憶する鍵を消去することを特徴とする。

また、本発明は、利用不可状態のコンテンツを保持する第 1 の端末装置が、第 2 の端末装置から前記コンテンツを利用可能状態にするために必要なデータを読み出し、前記第 1 の端末装置のコンテンツを利用可能状態にする著作権保護システムであって、前記第 1 の端末装置は、第 1 の暗号化されたコンテンツを記憶する第 1 の記憶部と、前記第 1 のコンテンツを復号するための鍵を記憶する第 1 の鍵記憶部を備え、前記第 2 の端末装置は、前記第 1 の暗号化されたコンテンツを復号するために必要なデータを記憶するデータ記憶部

を備え、前記第1の端末装置は、前記第2の端末装置から前記データ記憶部に記憶するデータを受信して、前記受信したデータに基づいて、前記第1の記憶部に記憶する暗号化コンテンツを復号するために必要な鍵を獲得して、前記第1の鍵記憶部に前記鍵を記憶することを特徴とする。

【0029】

また、本発明は、前記著作権保護システムであって、前記第1の端末装置は、前記端末装置固有の鍵を記憶する第2の鍵記憶部を備え、前記第2の端末装置の前記データ記憶部に記憶するデータは、前記第1の記憶部に記憶する鍵を、前記第2の鍵記憶部に記憶する鍵を用いて暗号化したデータであることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記第1の端末装置は、コンテンツに埋め込まれた鍵を抽出する抽出部を備え、前記第2の端末装置の前記データ記憶部に記憶するデータは、第2の暗号化されたコンテンツ、並びに前記第2の暗号化されたコンテンツを復号するための鍵であり、さらに、前記第2の暗号化されたコンテンツには、前記第1のコンテンツを復号するための鍵が埋め込まれていることを特徴とする。

【0030】

また、本発明は、前記著作権保護システムであって、前記第2の端末装置の前記データ記憶部に記憶するデータは、前記第1の暗号化されたコンテンツを復号するための鍵であることを特徴とする。

【発明の効果】

【0031】

本発明によれば、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツを復号するための鍵も合わせて移動させることにより、記録再生装置内のコンテンツを消去することなく無効化することが可能となり、移動したコンテンツを再び当該記録再生装置へ戻す場合に、前記復号鍵を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にすることが可能となる。

【発明を実施するための最良の形態】

【0032】

以下、本発明の実施の形態について、図面を参照しながら説明する。図1は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツを供給するコンテンツ供給装置101と、前記コンテンツを獲得して、コンテンツの記録、並びに再生を行い、さらにコンテンツの移動を実行する記録再生装置102と、前記移動するコンテンツを獲得する記録再生装置103、あるいは可搬媒体104からなる。

【0033】

前記記録再生装置102は、前記コンテンツ供給装置101からコンテンツを受信して記録する際、当該コンテンツを暗号化して、例えば内蔵HDDに記録する。そして、当該コンテンツを移動する際は、移動先となる装置、あるいは可搬媒体が正規装置、あるいは正規可搬媒体であるか否かを確認（認証）した上で、コンテンツの移動を実行する。さらに、前記記録再生装置102は、コンテンツの移動が完了した後に、内部に記録するコンテンツを利用できない状態にする。ここで、認証技術は、例えばDTP規格で定められた手順に従う、あるいは非特許文献1、並びに非特許文献2に開示される公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。

【0034】

（実施の形態1）

図2は、本発明の実施の形態1における、記録再生装置102が可搬媒体104にコンテンツを移動させる場合の記録再生装置102、並びに可搬媒体104の機能を示す機能ブロック図である。

記録再生装置102は、外部からのコンテンツを受信するコンテンツ受信部201と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部202と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部203と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部204と、前記装

置記録鍵を用いて、前記暗号化したコンテンツを復号する復号部205と、前記復号したコンテンツを（圧縮）変換する変換部206と、前記変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部207と、前記生成した媒体記録鍵を記憶する媒体記録鍵記憶部208と、前記媒体記録鍵を用いて、前記変換したコンテンツを暗号化する暗号化部209と、前記暗号化したコンテンツ、前記媒体記録鍵、並びに前記装置記録鍵を可搬媒体104に書き込む、あるいは可搬媒体104から読み出す書込／読出部210を備える。前記装置記録鍵記憶部202、並びに媒体記録鍵記憶部208に記憶する各鍵データは、書込／読出部210を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

【0035】

また、可搬媒体104は、暗号化コンテンツを記録する暗号化コンテンツ領域221と、媒体記録鍵を記録する媒体記録鍵領域222と、装置記録鍵を記録する装置記録鍵領域223を備える。前記可搬媒体104が備える前記媒体記録鍵領域222、並びに装置記録鍵領域223は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

【0036】

次に、図3を用いて、記録再生装置102から、可搬媒体104へコンテンツを移動する場合の動作について説明する。また、図4は、記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。

S301：記録再生装置102は、媒体記録鍵生成部207において媒体記録鍵を生成して、媒体記録鍵記憶部208に、前記生成した媒体記録鍵を記憶する。データの記録状態を図4（a）に示す。

【0037】

S302：記録再生装置102は、暗号化コンテンツ記録部204に記録する暗号化コンテンツを読み出し、復号部205において、装置記録鍵記憶部202に記憶する装置記録鍵を用いて、前記読み出した暗号化コンテンツを復号する。

S303：記録再生装置102は、変換部206において、S302で復号したコンテンツを（圧縮）変換する。

【0038】

S304：記録再生装置102は、暗号化部209において、S301で生成／記憶した媒体記録鍵を用いて、S303で変換したコンテンツを暗号化する。

S305：記録再生装置102は、S304で暗号化したコンテンツを、書込／読出部210を介して可搬媒体104の暗号化コンテンツ領域221へ記録する。データの記録状態を図4（b）に示す。

【0039】

S306：記録再生装置102は、装置記録鍵記憶部202に記憶する装置記録鍵を、書込／読出部210を介して可搬媒体104の装置記録鍵領域223へ記録する。

S307：記録再生装置102は、装置記録鍵記憶部202に記憶する装置記録鍵を消去する。データの記録状態を図4（c）に示す。

S308：記録再生装置102は、媒体記録鍵記憶部208に記憶する媒体記録鍵を、書込／読出部210を介して可搬媒体104の媒体記録鍵領域222へ記録する。

【0040】

S309：記録再生装置102は、媒体記録鍵記憶部208に記憶する媒体記録鍵を消去する。データの記録状態を図4（d）に示す。

次に、図5を用いて、可搬媒体104から、記録再生装置102へコンテンツを移動する場合の動作について説明する。また、図6は、記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。ただし、図6（a）は、コンテンツ移動前の初期状態を示す図である。

【0041】

S501：可搬媒体104は、暗号化コンテンツ領域221に記録する暗号化コンテ

ッ、並びに媒体記録鍵領域 222 に記録する媒体記録鍵を消去する。データの記録状態を図 6 (b) に示す。

S502: 記録再生装置 102 は、可搬媒体 104 の装置記録鍵領域 223 に記録する装置記録鍵を書込／読出部 210 を介して読み出し、装置記録鍵記憶部 202 に記憶する。

【0042】

S503: 可搬媒体 104 は、装置記録鍵領域 223 に記憶する装置記録鍵を消去する。データの記録状態を図 6 (c) に示す。

(実施の形態 2)

図 7 は、本発明の実施の形態 2 における、記録再生装置 102 が可搬媒体 104 にコンテンツを移動させる場合の記録再生装置 102、並びに可搬媒体 104 の機能を示す機能ブロック図である。なお、図 7 において、実施の形態 1 における記録再生装置 102 および可搬媒体 104 と同一の構成要素については、同一の符号を付すものとする。

【0043】

記録再生装置 102 は、外部からのコンテンツを受信するコンテンツ受信部 201 と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部 202 と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部 203 と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部 204 と、前記装置記録鍵を用いて、前記暗号化したコンテンツを復号する復号部 205 と、前記復号したコンテンツを（圧縮）変換する変換部 206 と、前記変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部 207 と、前記生成した媒体記録鍵を記憶する媒体記録鍵記憶部 208 と、前記媒体記録鍵を用いて、前記変換したコンテンツを暗号化する暗号化部 209 と、装置記録鍵を暗号化するために用いる装置固有鍵を記憶する装置固有鍵記憶部 701 と、前記装置固有鍵を用いて、前記装置記録鍵を暗号化、あるいは復号する暗号化／復号部 702 と、前記暗号化したコンテンツ、前記媒体記録鍵、並びに前記暗号化した装置記録鍵を可搬媒体 104 に書き込む、あるいは可搬媒体 104 から読み出す書込／読出部 210 を備える。前記装置記録鍵記憶部 202、並びに媒体記録鍵記憶部 208 に記憶する各鍵データは、書込／読出部 210 を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

【0044】

また、可搬媒体 104 は、暗号化コンテンツを記録する暗号化コンテンツ領域 221 と、媒体記録鍵を記録する媒体記録鍵領域 222 と、暗号化装置記録鍵を記録する暗号化装置記録鍵領域 703 を備える。前記可搬媒体 104 が備える前記媒体記録鍵領域 222 は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

【0045】

次に、図 8 を用いて、記録再生装置 102 から、可搬媒体 104 へコンテンツを移動する場合の動作について説明する。また、図 9 は、記録再生装置 102、並びに可搬媒体 104 における各データの記録状態を示した図である。

S801: 記録再生装置 102 は、媒体記録鍵生成部 207 において媒体記録鍵を生成して、媒体記録鍵記憶部 208 に、前記生成した媒体記録鍵を記憶する。データの記録状態を図 9 (a) に示す。

【0046】

S802: 記録再生装置 102 は、暗号化コンテンツ記録部 204 に記録する暗号化コンテンツを読み出し、復号部 205 において、装置記録鍵記憶部 202 に記憶する装置記録鍵を用いて、前記読み出した暗号化コンテンツを復号する。

S803: 記録再生装置 102 は、変換部 206 において、S802 で復号したコンテンツを（圧縮）変換する。

【0047】

S804: 記録再生装置 102 は、暗号化部 209 において、S801 で生成／記憶し

た媒体記録鍵を用いて、S803で変換したコンテンツを暗号化する。

S805:記録再生装置102は、S804で暗号化したコンテンツを、書込/読出部210を介して可搬媒体104の暗号化コンテンツ領域221へ記録する。データの記録状態を図9(b)に示す。

【0048】

S806:記録再生装置102は、暗号化/復号部702において、装置固有鍵記憶部701に記憶する装置用固有鍵を用いて、装置記録鍵を暗号化して、書込/読出部210を介して可搬媒体104の暗号化装置記録鍵領域703に記録する。

S807:記録再生装置102は、装置記録鍵記憶部202に記憶する装置記録鍵を消去する。データの記録状態を図9(c)に示す。

【0049】

S808:記録再生装置102は、媒体記録鍵記憶部208に記憶する媒体記録鍵を、書込/読出部210を介して可搬媒体104の媒体記録鍵領域222へ記録する。

S809:記録再生装置102は、媒体記録鍵記憶部208に記憶する媒体記録鍵を消去する。データの記録状態を図9(d)に示す。

次に、図10を用いて、可搬媒体104から、記録再生装置102へコンテンツを移動する場合の動作について説明する。また、図11は、記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。ただし、図11(a)は、コンテンツ移動前の初期状態を示す図である。

【0050】

S1001:可搬媒体104は、暗号化コンテンツ領域221に記録する暗号化コンテンツ、並びに媒体記録鍵領域222に記録する媒体記録鍵を消去する。データの記録状態を図11(b)に示す。

S1002:記録再生装置102は、可搬媒体104の暗号化装置記録鍵領域703に記録する暗号化装置記録鍵を書込/読出部210を介して読み出して、暗号化/復号部702において、装置固有鍵記憶部701に記憶する装置固有鍵を用いて、暗号化装置記録鍵を復号して、装置記録鍵記憶部202に記憶する。

【0051】

S1003:可搬媒体104は、暗号化装置記録鍵領域503に記憶する暗号化装置記録鍵を消去する。データの記録状態を図11(c)に示す。

(実施の形態3)

図12は、本発明の実施の形態3における、記録再生装置102が可搬媒体104にコンテンツを移動させる場合の記録再生装置102、並びに可搬媒体104の機能を示す機能ブロック図である。なお、図12において、実施の形態1における記録再生装置102および可搬媒体104と同一の構成要素については、同一の符号を付すものとする。

【0052】

記録再生装置102は、外部からのコンテンツを受信するコンテンツ受信部201と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部202と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部203と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部204と、前記装置記録鍵を用いて、前記暗号化したコンテンツを復号する復号部205と、前記復号したコンテンツを(圧縮)変換する変換部206と、前記変換したコンテンツに対して前記装置記録鍵を埋め込む、あるいは抽出する鍵埋込/抽出部1201と、前記鍵を埋め込んだコンテンツを暗号化、あるいは復号するために用いる媒体記録鍵を生成する媒体記録鍵生成部207と、前記生成した媒体記録鍵を記憶する媒体記録鍵記憶部208と、前記媒体記録鍵を用いて、前記鍵を埋め込んだコンテンツを暗号化、あるいは復号する暗号化/復号部1202と、前記暗号化したコンテンツ、及び前記媒体記録鍵を可搬媒体104に書き込む、あるいは可搬媒体104から読み出す書込/読出部210を備える。前記装置記録鍵記憶部202、並びに媒体記録鍵記憶部208に記憶する各鍵データは、書込/読出部210を介して当該データが媒体に書き込まれた後は、そのデータが消去される。

【0053】

また、可搬媒体104は、暗号化コンテンツを記録する暗号化コンテンツ領域221と、媒体記録鍵を記録する媒体記録鍵領域222を備える。前記可搬媒体104が備える前記媒体記録鍵領域222は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

次に、図13を用いて、記録再生装置102から、可搬媒体104へコンテンツを移動する場合の動作について説明する。また、図14は、記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。

【0054】

S1301:記録再生装置102は、媒体記録鍵生成部207において媒体記録鍵を生成して、媒体記録鍵記憶部208に、前記生成した媒体記録鍵を記憶する。データの記録状態を図14(a)に示す。

S1302:記録再生装置102は、暗号化コンテンツ記録部に記録する暗号化コンテンツを読み出し、復号部205において、装置記録鍵記憶部202に記憶する装置記録鍵を用いて、前記読み出した暗号化コンテンツを復号する。

【0055】

S1303:記録再生装置102は、変換部206において、S1302で復号したコンテンツを(圧縮)変換する。

S1304:記録再生装置102は、鍵埋込/抽出部1201において、S1303で変換したコンテンツに装置記録鍵を埋め込み、暗号化/復号部1202において、S1301で生成/記憶した媒体記録鍵を用いて、鍵を埋め込んだコンテンツを暗号化する。

【0056】

S1305:記録再生装置102は、S1304で暗号化したコンテンツを、書込/読出部210を介して可搬媒体104の暗号化コンテンツ領域221へ記録する。データの記録状態を図14(b)に示す。

S1306:記録再生装置102は、装置記録鍵記憶部202に記憶する装置記録鍵を消去する。データの記録状態を図14(c)に示す。

【0057】

S1307:記録再生装置102は、媒体記録鍵記憶部208に記憶する媒体記録鍵を、書込/読出部210を介して可搬媒体104の媒体記録鍵領域222へ記録する。

S1308:記録再生装置102は、媒体記録鍵記憶部208に記憶する媒体記録鍵を消去する。データの記録状態を図14(d)に示す。

次に、図15を用いて、可搬媒体104から、記録再生装置102へコンテンツを移動する場合の動作について説明する。また、図16は、記録再生装置102、並びに可搬媒体104における各データの記録状態を示した図である。ただし、図16(a)は、コンテンツ移動前の初期状態を示す図である。

S1501:記録再生装置102は、可搬媒体104の暗号化コンテンツ領域221に記録する暗号化コンテンツ、並びに媒体記録用領域222に記録する媒体記録鍵を書込/読出部210を介して読み出す。

【0058】

S1502:可搬媒体104は、暗号化コンテンツ領域221に記録する暗号化コンテンツ、並びに媒体記録鍵領域222に記録する媒体記録鍵を消去する。データの記録状態を図16(b)に示す。

S1503:記録再生装置102は、暗号化/復号部1202において、S1501で読み出した媒体記録鍵を用いて、同じくS1501で読み出した暗号化コンテンツを復号し、さらに、鍵埋込/抽出部1201において、復号したコンテンツから装置記録鍵を抽出して、装置記録鍵記憶部202に記憶する。データの記録状態を図16(c)に示す。

【0059】

(実施の形態4)

図17は、本発明の実施の形態4における、記録再生装置102が可搬媒体104にコ

ンテンツを移動させる場合の記録再生装置 102、並びに可搬媒体 104 の機能を示す機能ブロック図である。なお、図 17 において、実施の形態 1 における記録再生装置 102 および可搬媒体 104 と同一の構成要素については、同一の符号を付すものとする。

【0060】

記録再生装置 102 は、外部からのコンテンツを受信するコンテンツ受信部 201 と、前記受信したコンテンツを暗号化するために用いるコンテンツ鍵を記憶するコンテンツ鍵記憶部 1701 と、前記コンテンツ鍵を用いて、前記受信したコンテンツを暗号化する暗号化部 203 と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部 204 と、前記コンテンツ鍵を用いて、前記暗号化したコンテンツを復号する復号部 205 と、前記復号したコンテンツを（圧縮）変換する変換部 206 と、前記コンテンツ鍵を用いて、前記変換したコンテンツを暗号化する暗号化部 209 と、前記暗号化したコンテンツ、前記媒体記録鍵、並びに前記コンテンツ鍵を可搬媒体 104 に書き込む、あるいは可搬媒体 104 から読み出す書込／読出部 210 を備える。前記コンテンツ鍵記憶部 1701 に記憶する鍵データは、書込／読出部 210 を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

【0061】

また、可搬媒体 104 は、暗号化コンテンツを記録する暗号化コンテンツ領域 221 と、コンテンツ鍵を記録するコンテンツ鍵領域 1702 を備える。前記可搬媒体 104 が備える前記コンテンツ鍵領域 1702 は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

次に、図 18 を用いて、記録再生装置 102 から、可搬媒体 104 へコンテンツを移動する場合の動作について説明する。また、図 19 は、記録再生装置 102、並びに可搬媒体 104 における各データの記録状態を示した図である。ただし、図 19 (a) は、コンテンツ移動前の初期状態を示す図である。

【0062】

S1801: 記録再生装置 102 は、暗号化コンテンツ記録部 204 に記録する暗号化コンテンツを読み出し、復号部 205 において、コンテンツ鍵記憶部 1701 に記憶するコンテンツ鍵を用いて、前記読み出した暗号化コンテンツを復号する。

S1802: 記録再生装置 102 は、変換部 206 において、S1801 で復号したコンテンツを（圧縮）変換する。

【0063】

S1803: 記録再生装置 102 は、暗号化部 209 において、コンテンツ鍵記憶部 1701 に記憶するコンテンツ鍵を用いて、S1802 で変換したコンテンツを暗号化する。

S1804: 記録再生装置 102 は、S1803 で暗号化したコンテンツを、書込／読出部 210 を介して可搬媒体 104 の暗号化コンテンツ領域 221 へ記録する。データの記録状態を図 19 (b) に示す。

【0064】

S1805: 記録再生装置 102 は、コンテンツ鍵 1701 に記憶するコンテンツ鍵を、書込／読出部 210 を介して可搬媒体 104 のコンテンツ鍵領域 1702 へ記録する。

S1806: 記録再生装置 102 は、コンテンツ鍵記憶部 1701 に記憶するコンテンツ鍵を消去する。データの記録状態を図 19 (c) に示す。

次に、図 20 を用いて、可搬媒体 104 から、記録再生装置 102 へコンテンツを移動する場合の動作について説明する。また、図 21 は、記録再生装置 102、並びに可搬媒体 104 における各データの記録状態を示した図である。ただし、図 21 (a) は、コンテンツ移動前の初期状態を示す図である。

【0065】

S2001: 可搬媒体 104 は、暗号化コンテンツ領域 221 に記録する暗号化コンテンツを消去する。データの記録状態を図 21 (b) に示す。

S2002: 記録再生装置 102 は、可搬媒体 104 のコンテンツ鍵領域 1702 に記

録するコンテンツ鍵を書込／読出部 210 を介して読み出し、コンテンツ鍵記憶部 170 1 に記憶する。

【0066】

S2003: 可搬媒体 104 は、コンテンツ鍵領域 1702 に記憶するコンテンツ鍵を消去する。データの記録状態を図 21 (c) に示す。

(その他の変形例)

(1) 本発明の実施の形態では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置から、別の記録再生装置へコンテンツを移動する構成であってもよい。

【0067】

(2) 本発明の実施の形態では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する際、記録再生装置、並びに可搬媒体に記録する各種データを消去する構成としたが、本発明はその構成に限定されるものではない。例えば、可搬媒体に記録する暗号化コンテンツは消去せずに、復号に必要な鍵だけを消去して、前記暗号化コンテンツを利用不可状態にする構成であってもよい。また、データの消去ではなく、データの一部を破壊して利用できない状態にする構成であってもよい。

【0068】

(3) 本発明の実施の形態において、記録再生装置が、コンテンツの移動処理における状態遷移を記憶する記憶部を備える構成であってもよい。記録再生装置は、コンテンツの移動が正しく完了しなかった場合、前記記憶部に記憶する状態遷移に基づいて、コンテンツの移動処理を続けて行うか、コンテンツの移動処理を最初からやり直すかを判断する構成であってもよい。さらに、記録再生装置は、前記記憶部に記憶する状態遷移を利用者に通知する通知部を備える構成であってもよい。その場合、正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、あるいはコンテンツの移動処理を最初からやり直すかを決定する構成であってもよい。

【0069】

(4) 本発明の実施の形態において、記録再生装置、並びに可搬媒体が、鍵を移動後に消去する場合、鍵の受信側が、鍵の送信側に対して正しく受信できたことを通知して、送信側は前記通知に基づいて受信を確認した後に、鍵を消去する構成であってもよい。

(5) 本発明の実施の形態において、コンテンツには当該コンテンツを一意に識別するための識別子が付与されており、可搬媒体に移動させたコンテンツを元の記録再生装置に戻す場合、前記記録再生装置は、自身が保持する暗号化コンテンツの識別子、並びに可搬媒体に記録する暗号化コンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。また、コンテンツには、コンテンツを一意に識別する識別子の代わりに、移動元の記録再生装置を一意に識別する識別子が付与されている構成であってもよい。この場合、記録再生装置は、コンテンツに付与されている記録再生装置の識別子と、自身の識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。

【0070】

(6) 本発明の実施の形態 4 では、コンテンツ鍵を暗号化せずに可搬媒体に記録する構成としたが、本発明はその構成に限定されるものではない。実施の形態 2 と同様に、装置固有鍵で暗号化して記録する構成であってもよい。

(7) 本発明の実施の形態 2 では、装置記録鍵を装置固有鍵で暗号化する構成としたが、本発明はその構成に限定されるものではない。例えば、装置固有鍵ではなく、複数の装置が共有する共有鍵で暗号化する構成でもよく、装置製造業者ごとに割り当てられる製造業者固有鍵で暗号化する構成であってもよい。また、暗号化するごとに鍵を生成して、前記生成した鍵で、前記装置記録鍵を暗号化する構成であってもよい。

【0071】

(8) 本発明の実施の形態では、コンテンツは外部のコンテンツ供給装置により供給される構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置に挿入された記録媒体からコンテンツを読み出す構成であってもよい。

【産業上の利用可能性】

【0072】

本発明にかかる著作権保護システムは、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツを復号するための鍵も合わせて移動させることにより、記録再生装置内のコンテンツを消去することなく利用不可状態にすることができ、移動したコンテンツを再び当該記録再生装置へ戻す場合に、前記復号するための鍵を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にできるという効果を有し、ユーザ利便性を損なわない著作権保護システムの実現において有用である。

【図面の簡単な説明】

【0073】

【図1】 本発明に係る著作権保護システムの全体構成を示すブロック図

【図2】 本発明の第1の実施の形態における機能ブロック図

【図3】 本発明の第1の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー

【図4】 本発明の第1の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図5】 本発明の第1の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー

【図6】 本発明の第1の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図7】 本発明の第2の実施の形態における機能ブロック図

【図8】 本発明の第2の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー

【図9】 本発明の第2の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図10】 本発明の第2の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー

【図11】 本発明の第2の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図12】 本発明の第3の実施の形態における機能ブロック図

【図13】 本発明の第3の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー

【図14】 本発明の第3の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図15】 本発明の第3の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー

【図16】 本発明の第3の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の各データの記録状態を示す図

【図17】 本発明の第4の実施の形態における機能ブロック図

【図18】 本発明の第4の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作フロー

【図19】 本発明の第4の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の各データの記録状態を示す図

【図20】 本発明の第4の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー

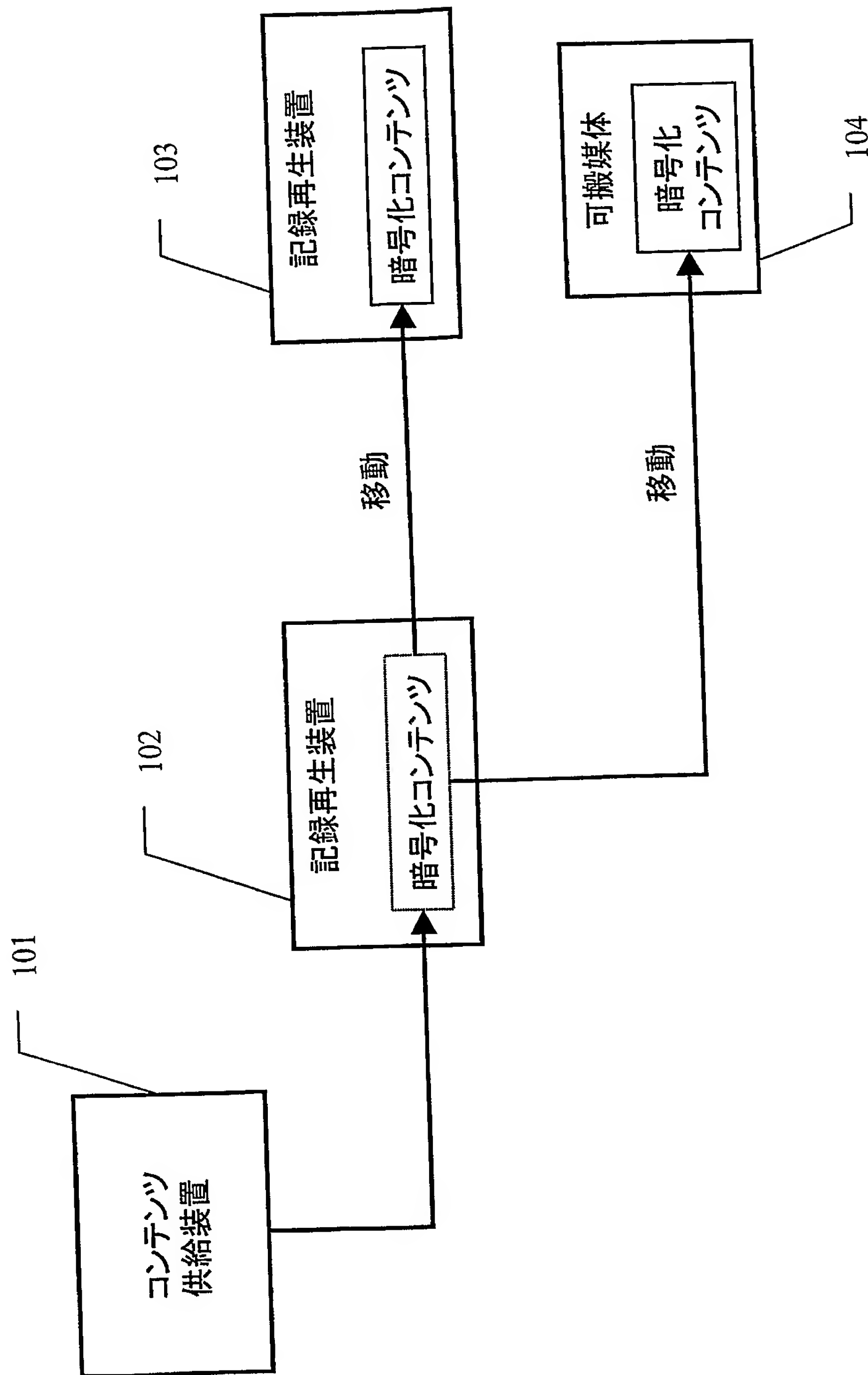
【図21】 本発明の第4の実施の形態における可搬媒体から記録再生装置へコンテンツ

ッを移動させる際の各データの記録状態を示す図
【符号の説明】

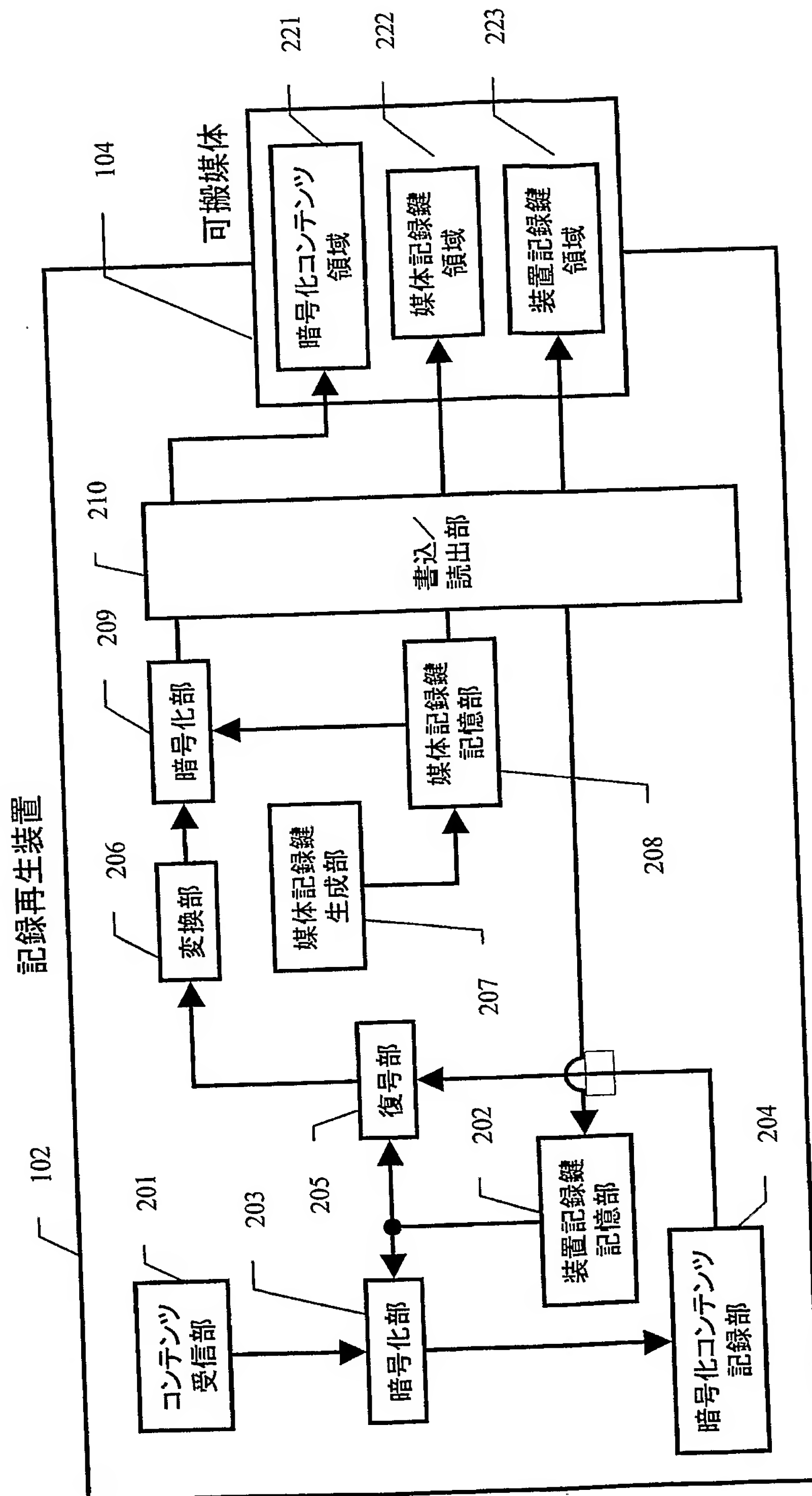
【 0 0 7 4 】

- 1 0 1 コンテンツ供給装置
- 1 0 2、1 0 3 記録再生装置
- 1 0 4 可搬媒体
- 2 0 1 コンテンツ受信部
- 2 0 2 装置記録鍵記憶部
- 2 0 3、2 0 9 暗号化部
- 2 0 4 暗号化コンテンツ記録部
- 2 0 5 復号部
- 2 0 6 変換部
- 2 0 7 媒体記録鍵生成部
- 2 0 8 媒体記録鍵記憶部
- 2 1 0 書込／読出部
- 2 2 1 暗号化コンテンツ領域
- 2 2 2 媒体記録鍵領域
- 2 2 3 装置記録鍵領域
- 7 0 1 装置固有鍵記憶部
- 7 0 2、1 2 0 2 暗号化／復号部
- 7 0 3 暗号化装置記録鍵領域
- 1 2 0 1 鍵埋込／抽出部
- 1 7 0 1 コンテンツ鍵記憶部
- 1 7 0 2 コンテンツ鍵領域

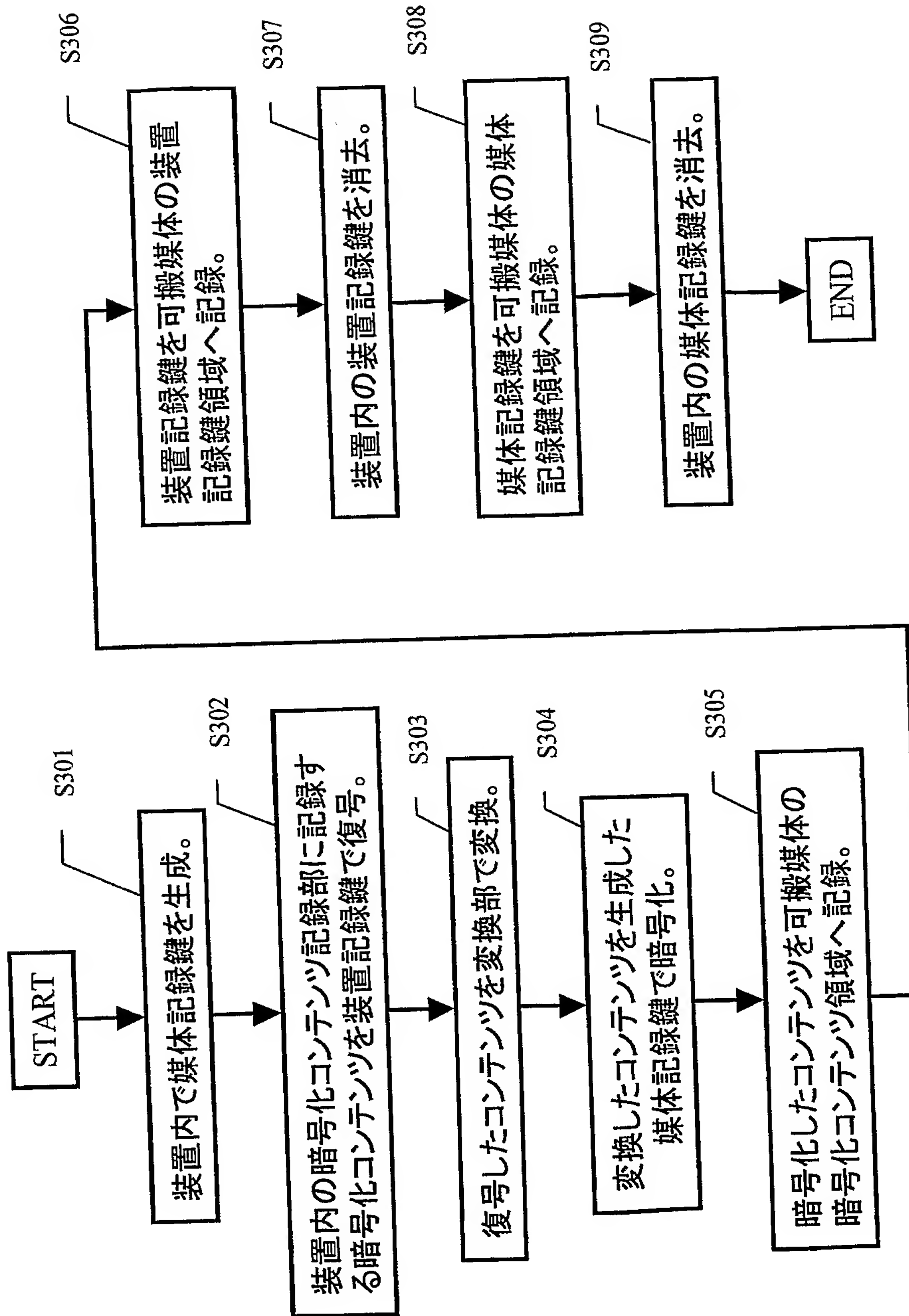
【書類名】 図面
【図 1】



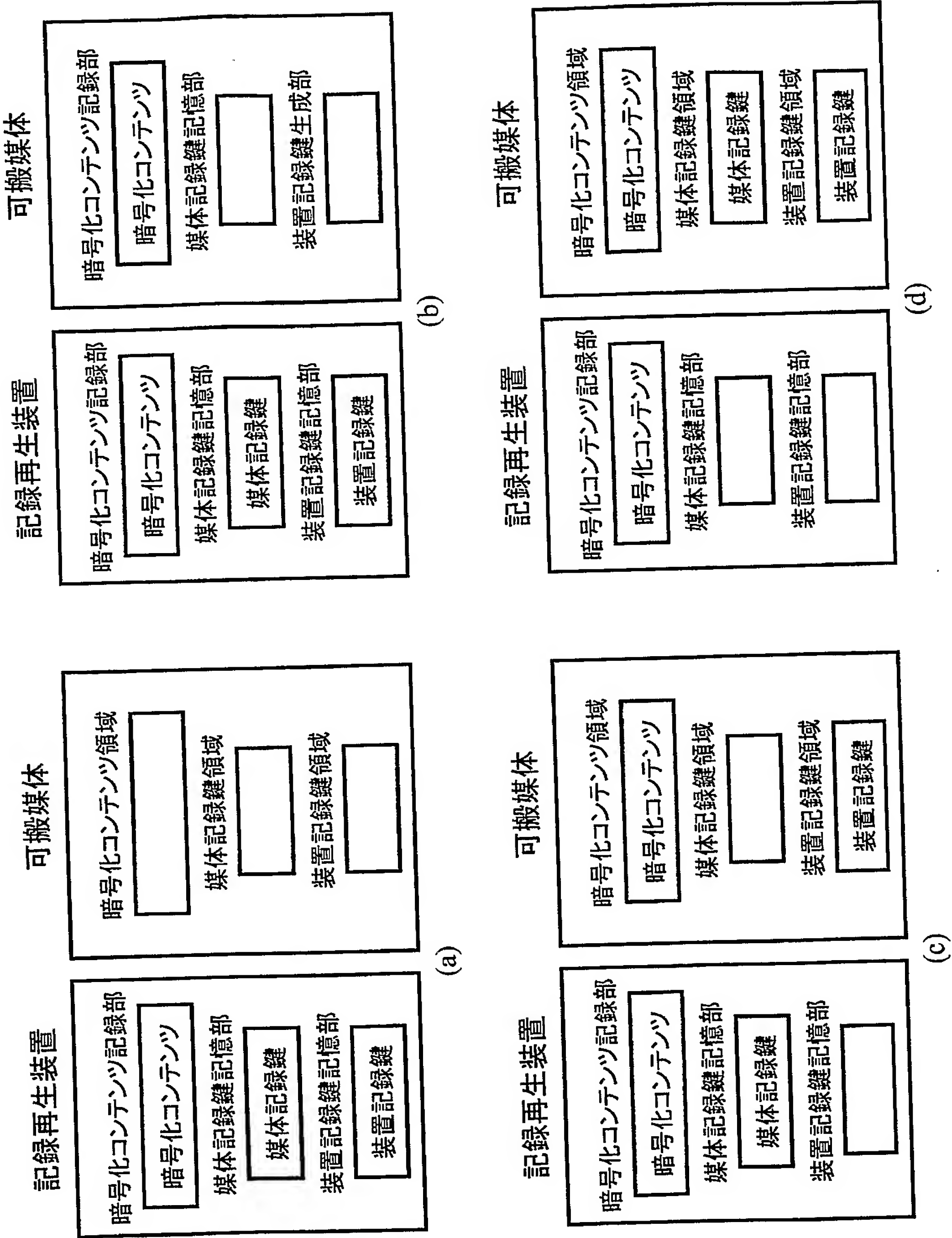
【図 2】



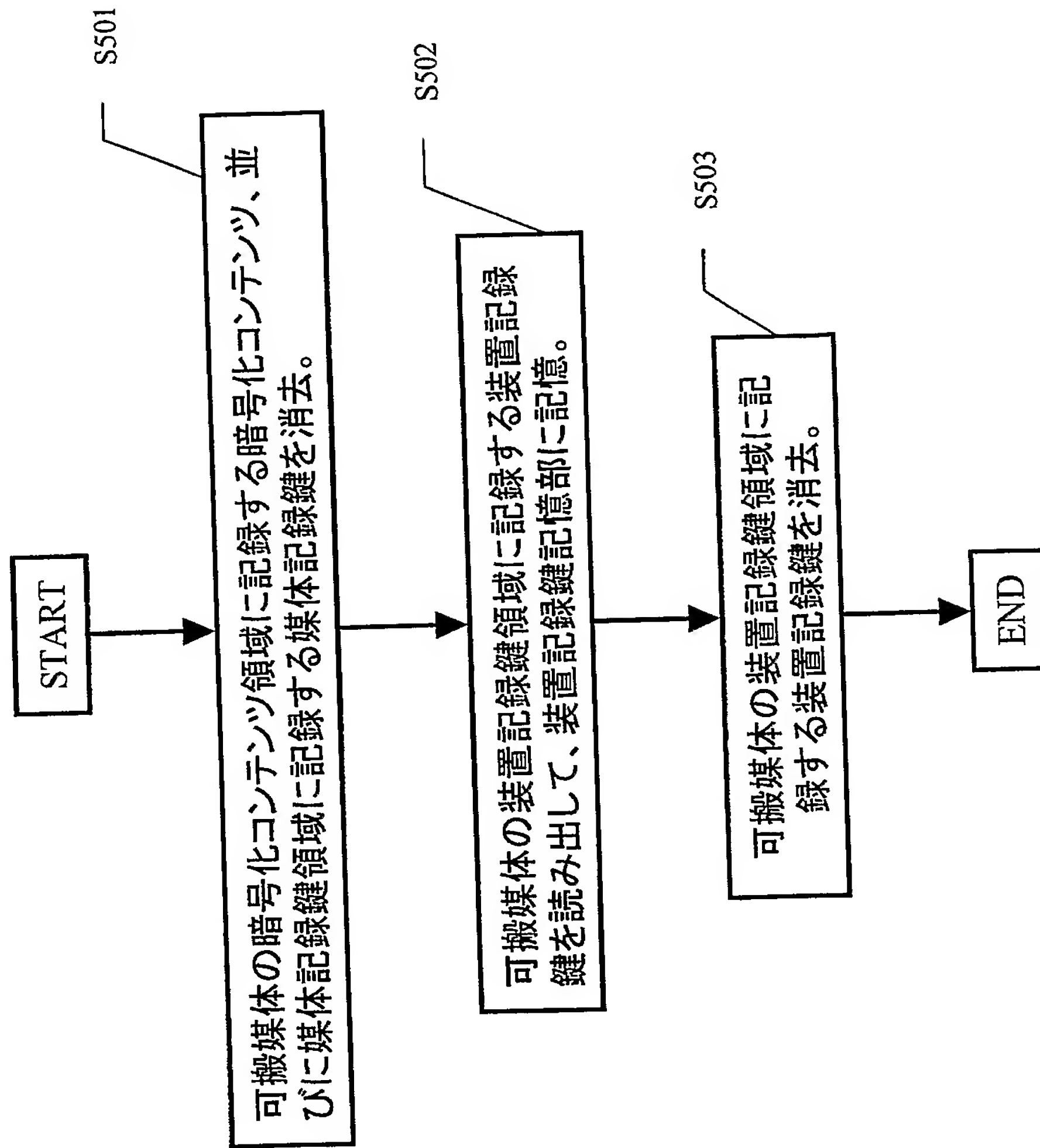
【図 3】



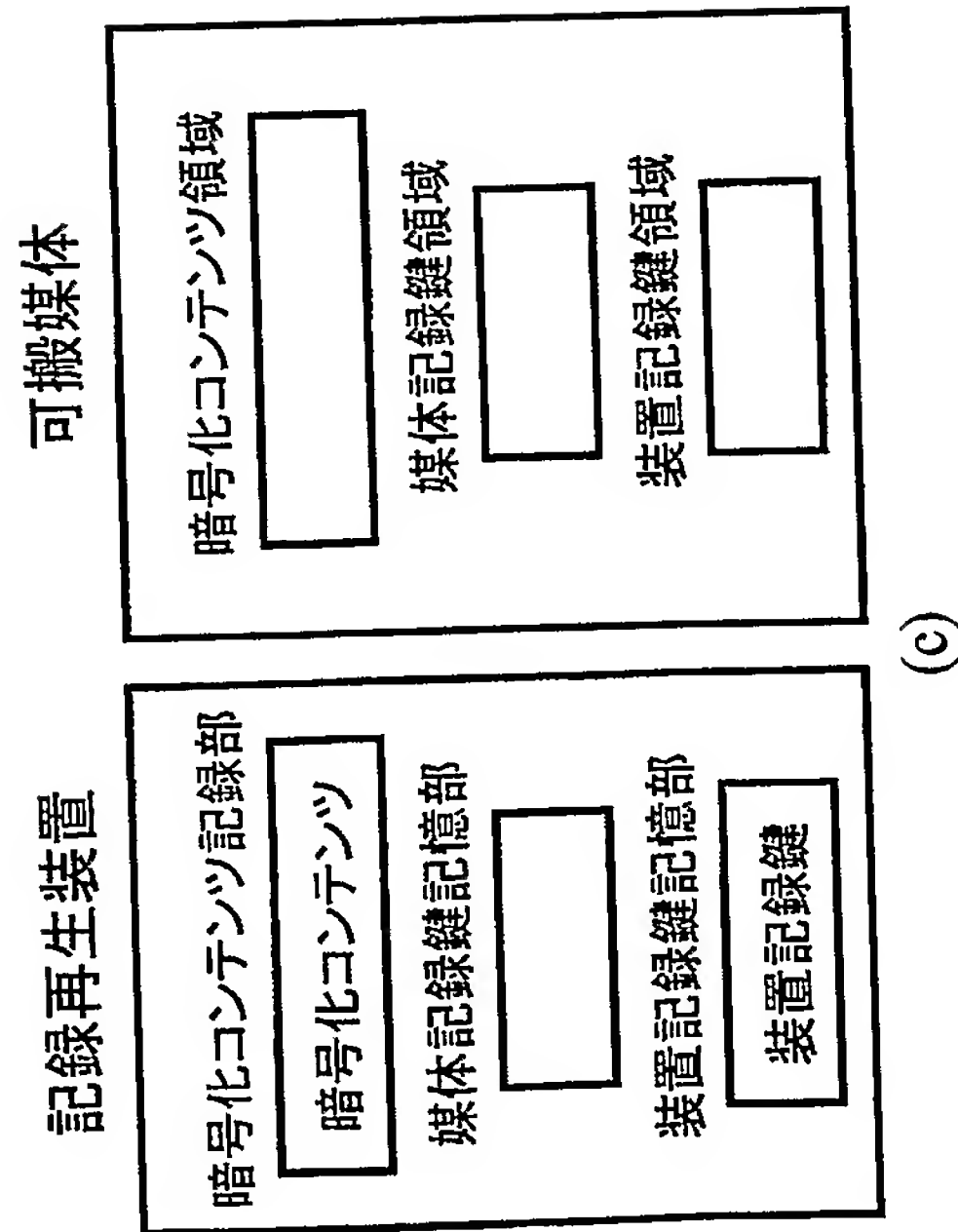
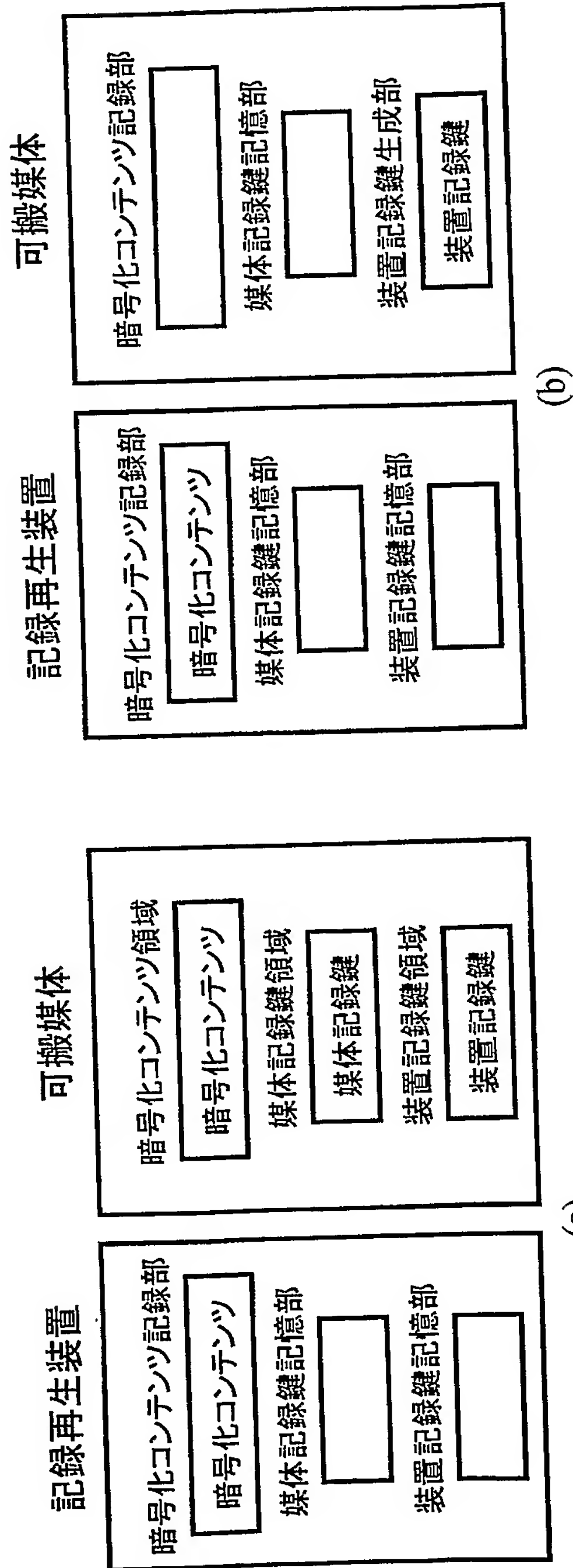
【図 4】



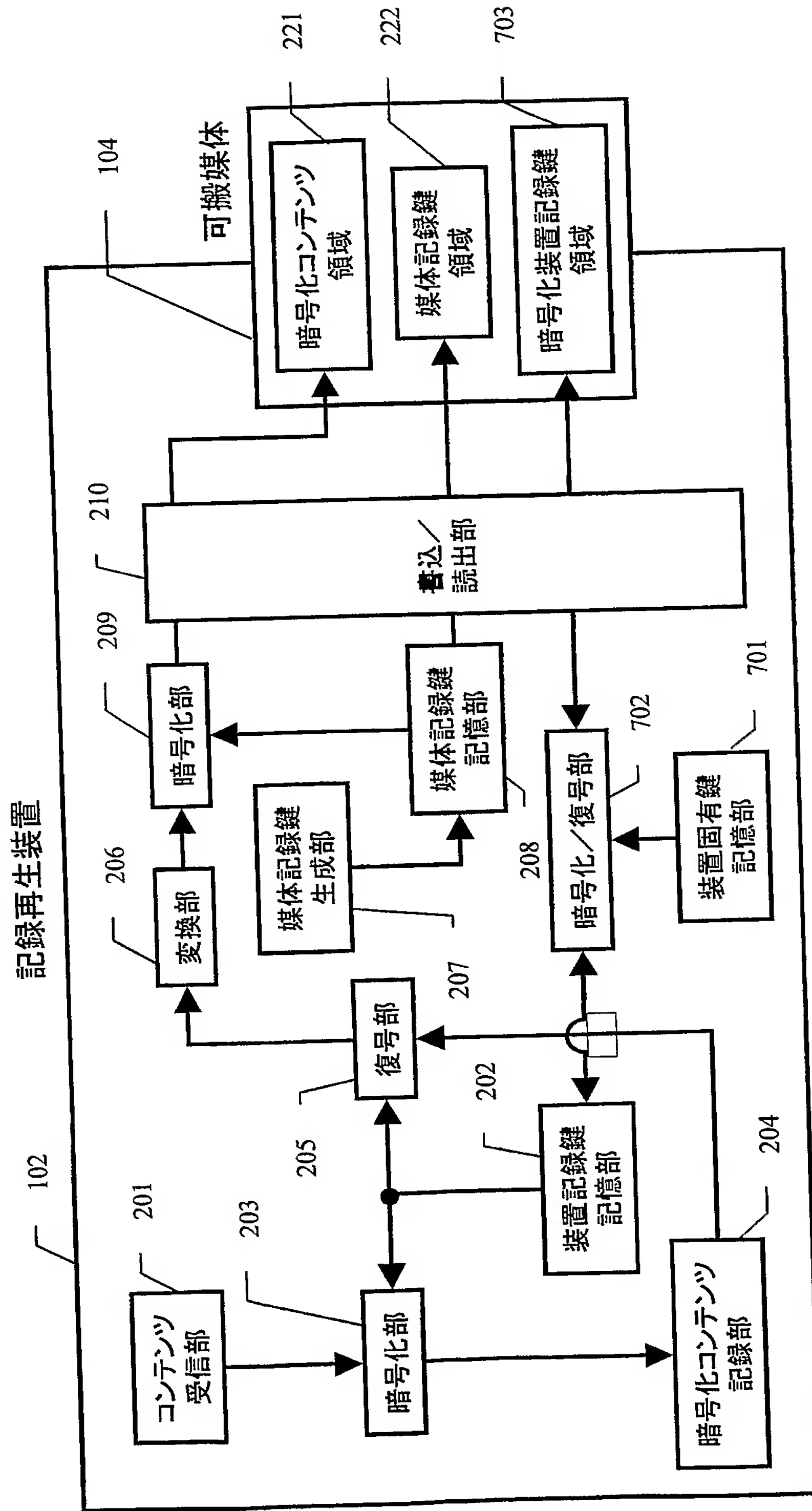
【図 5】



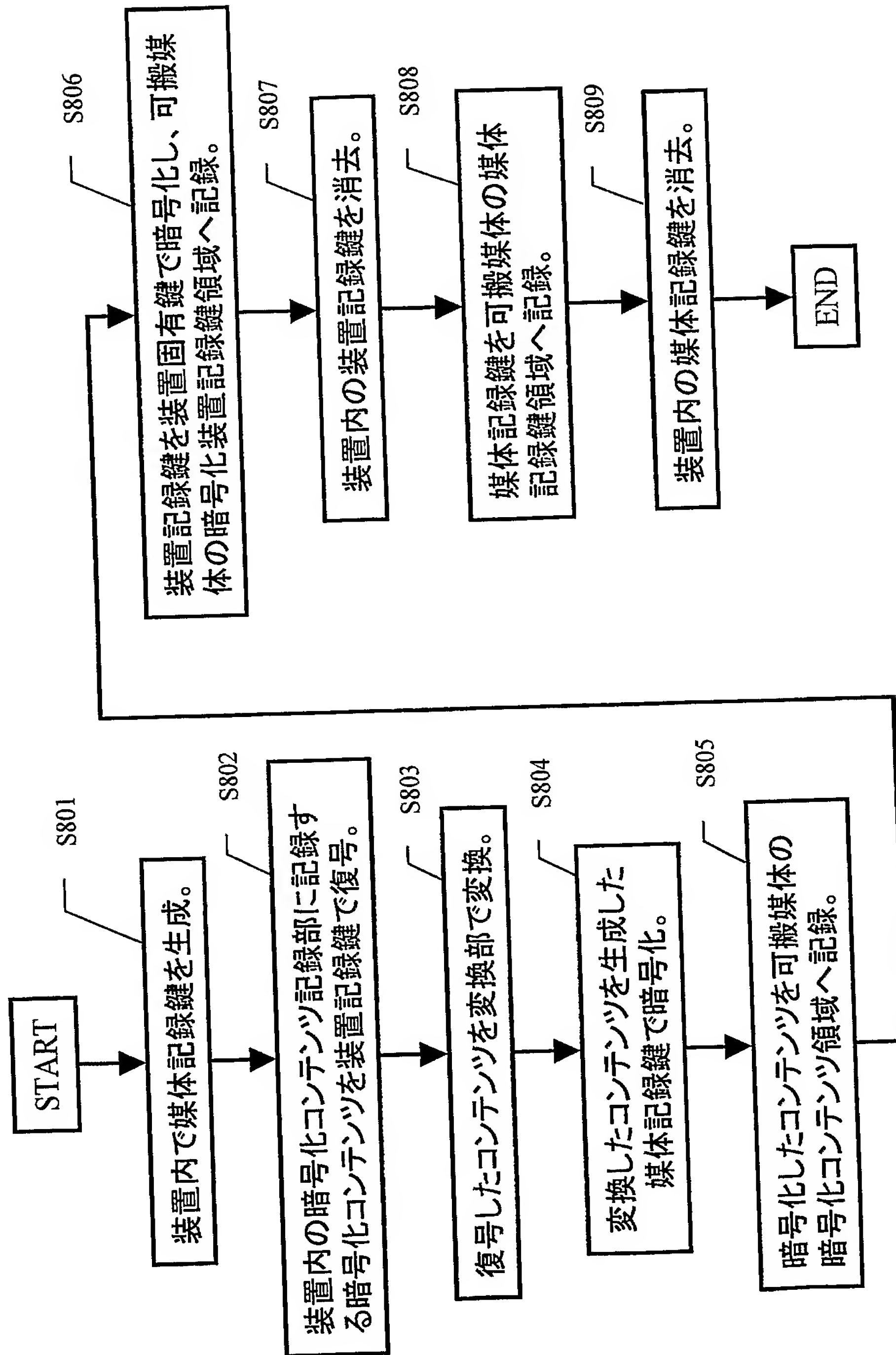
【図 6】



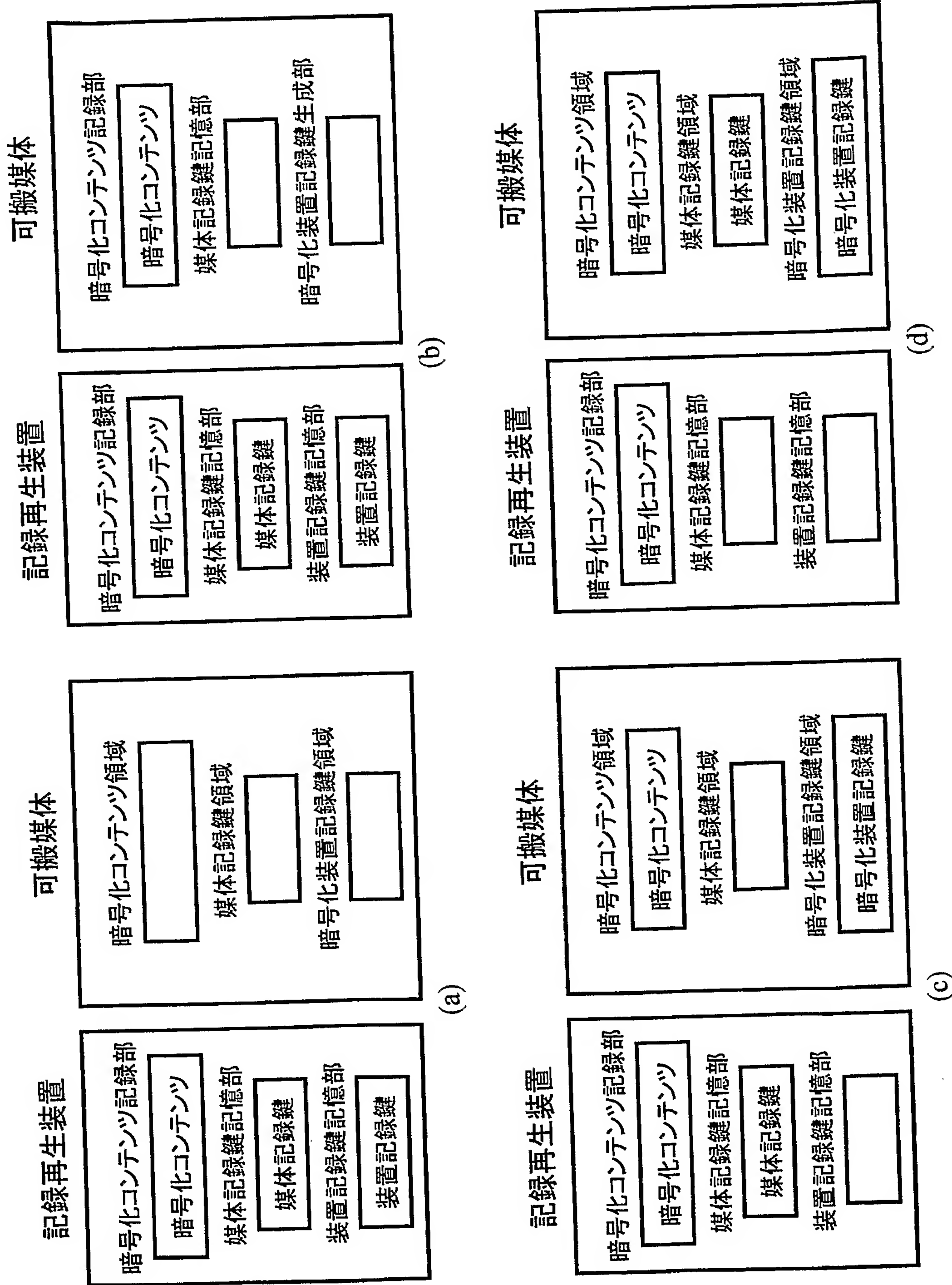
【図 7】



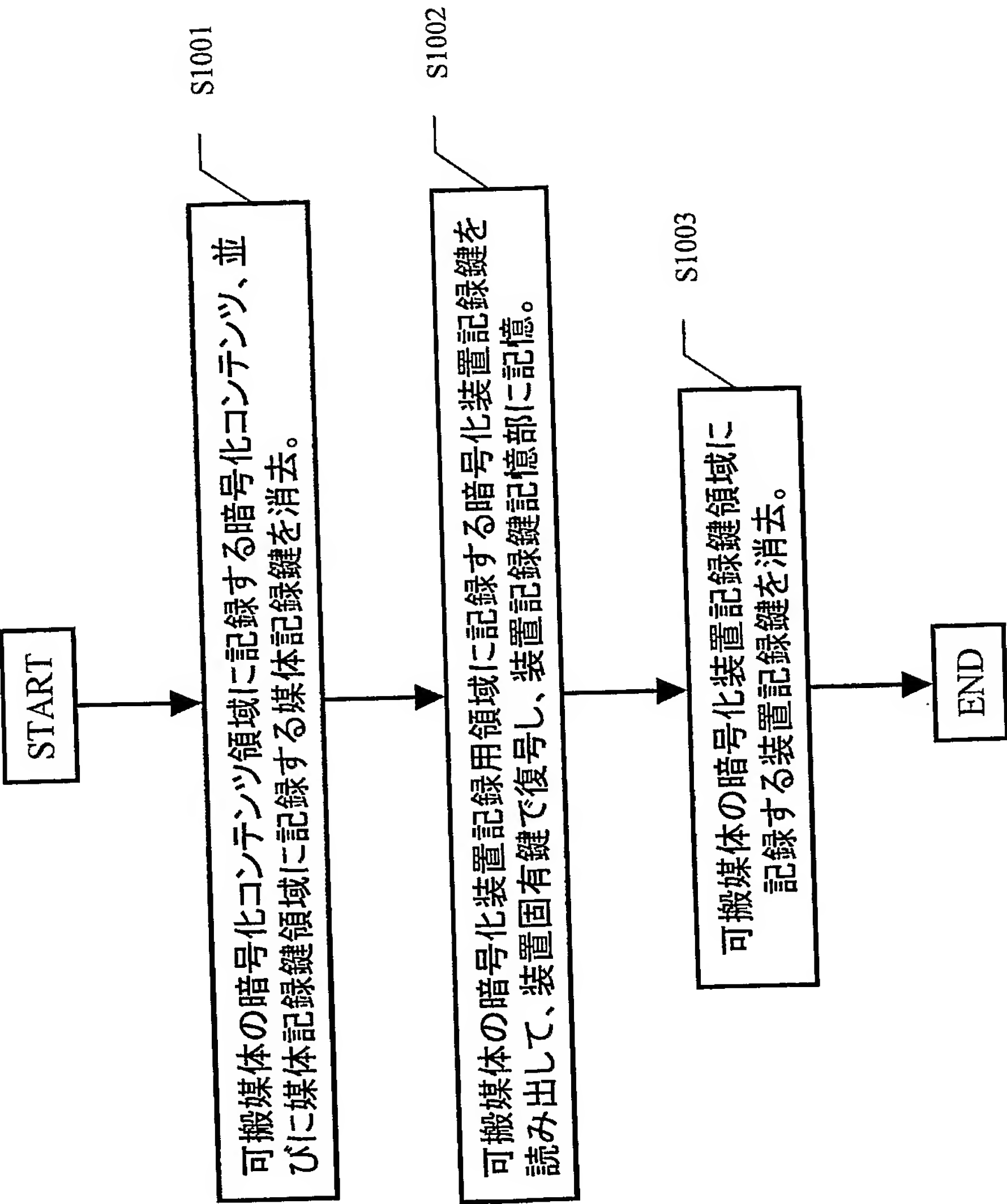
【図 8】



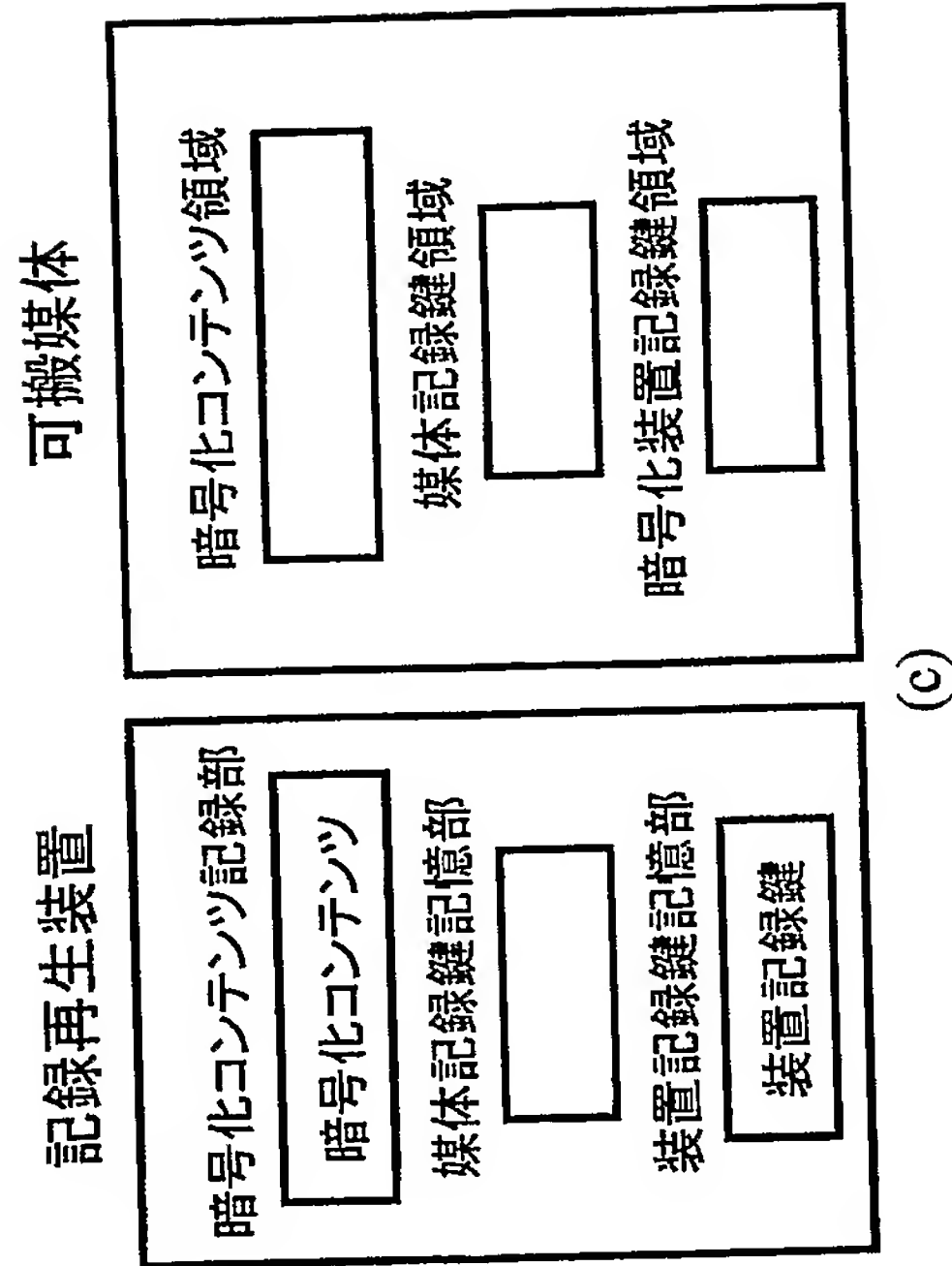
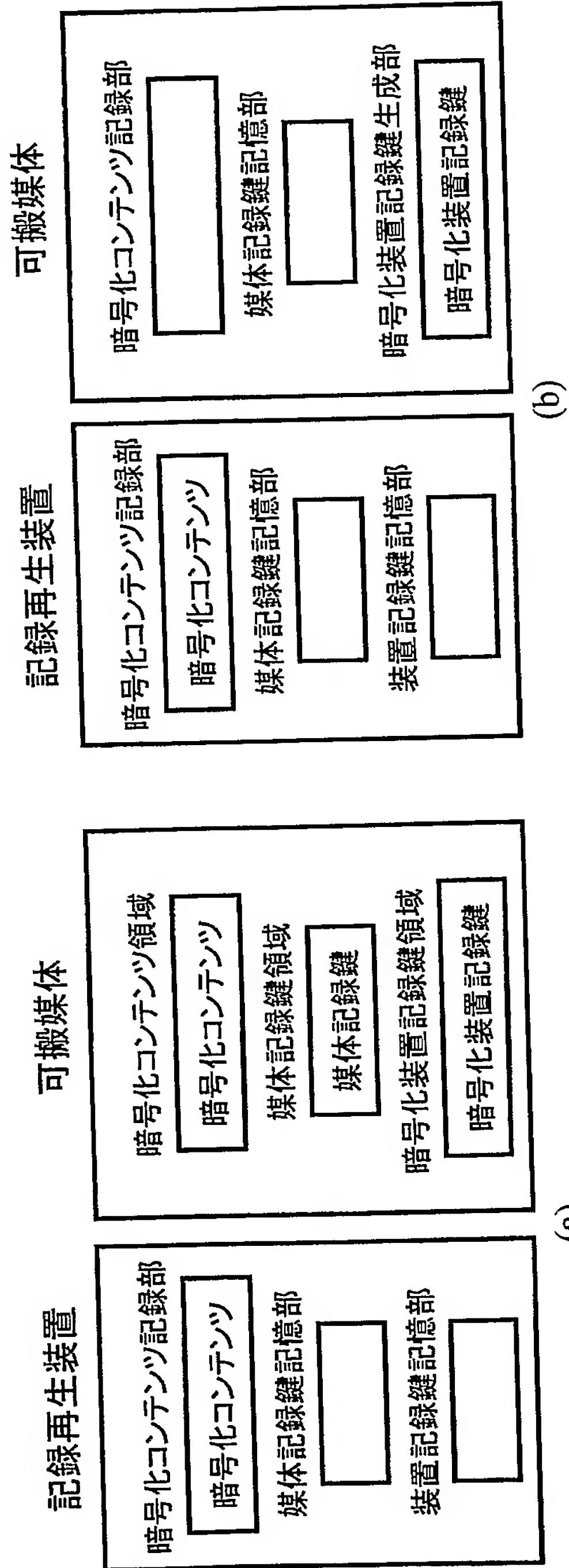
【図 9】



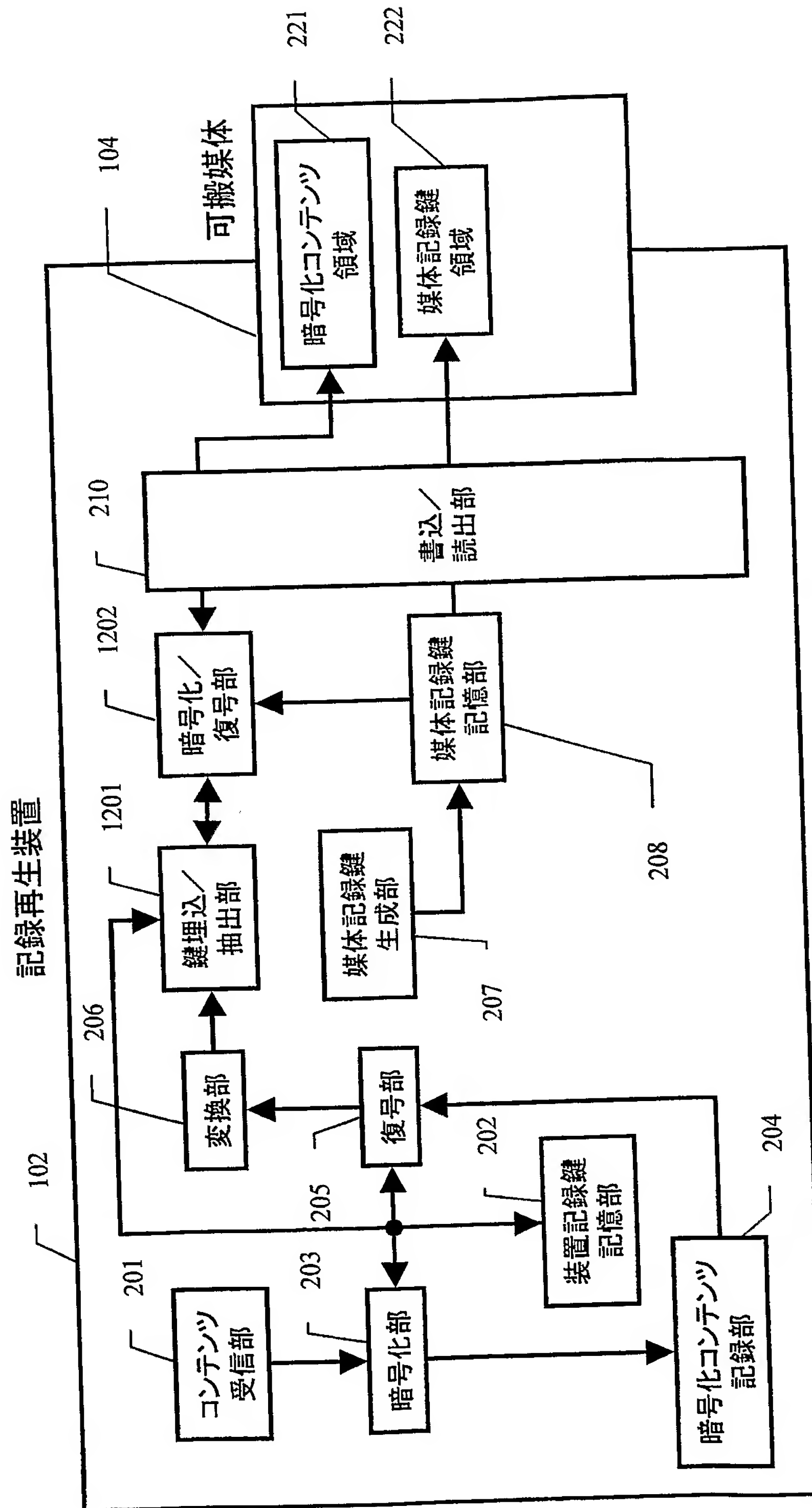
【図 10】



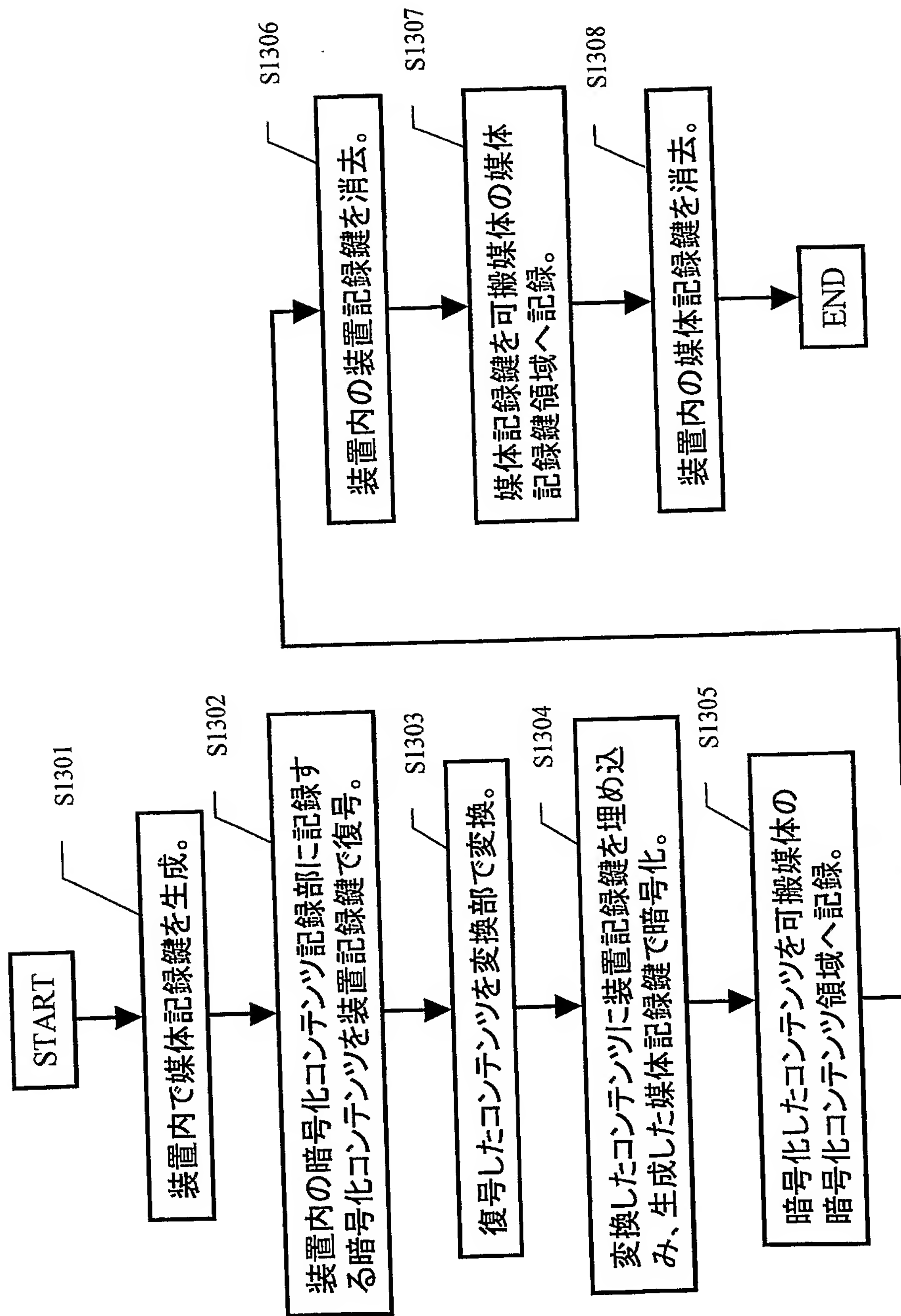
【図 11】



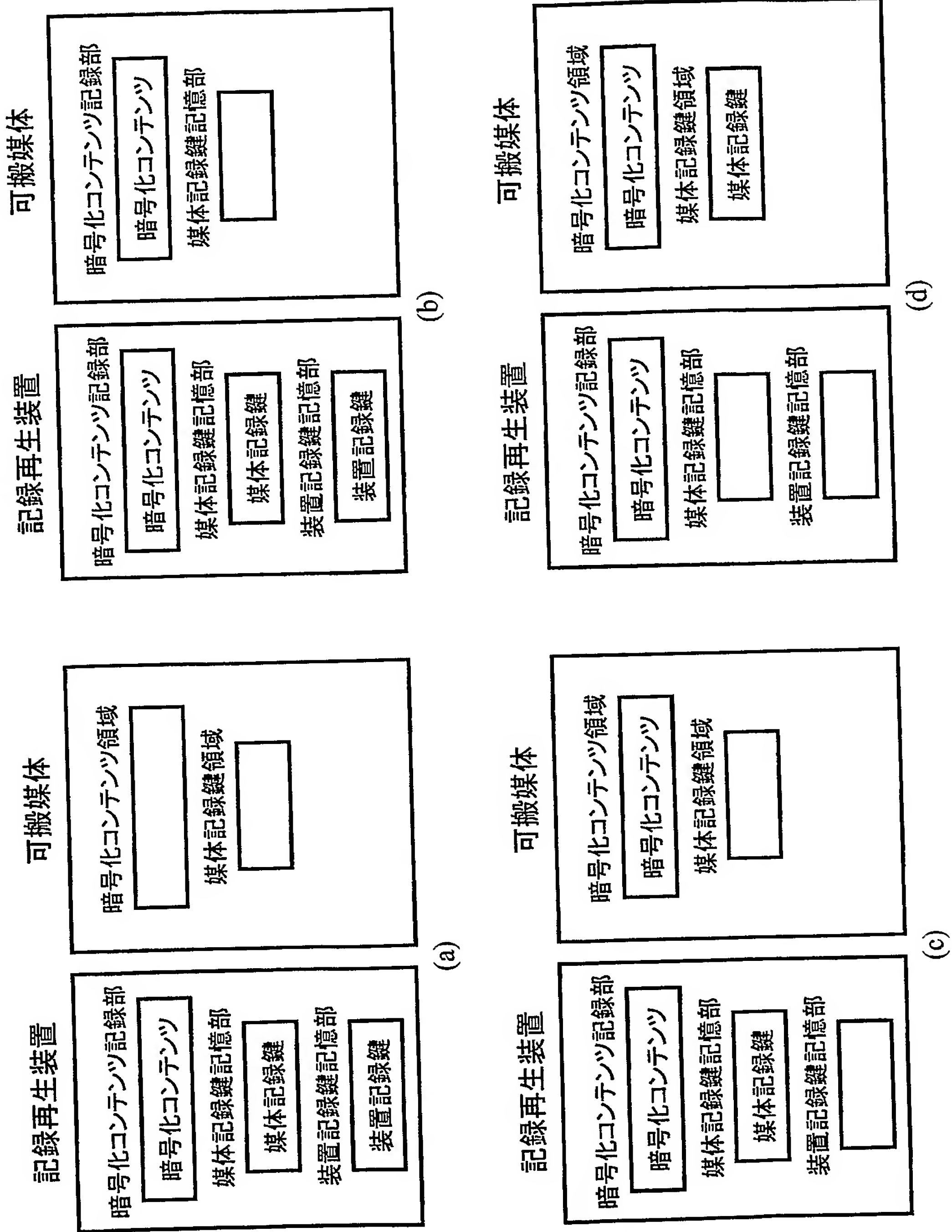
【図 12】



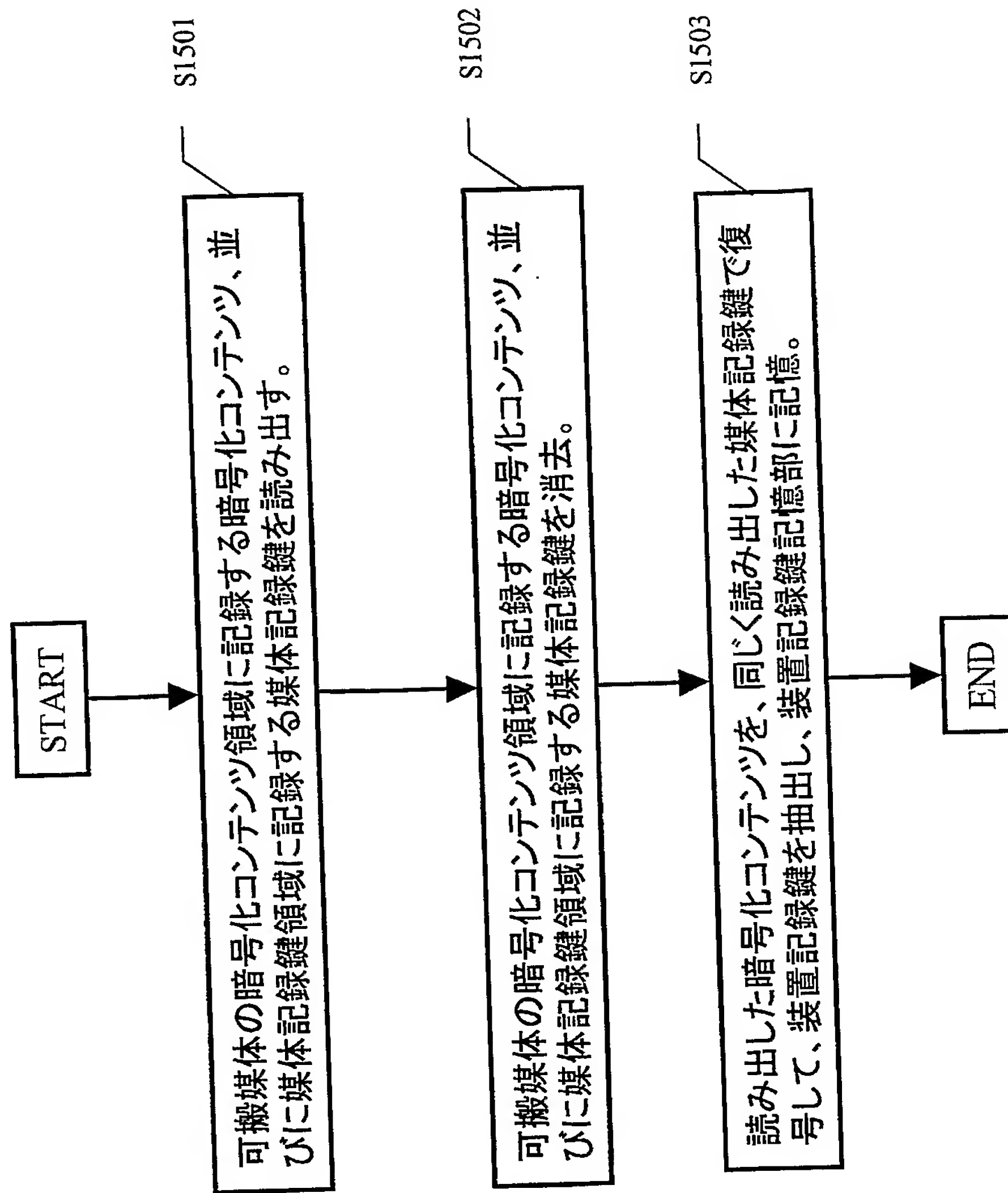
【図 13】



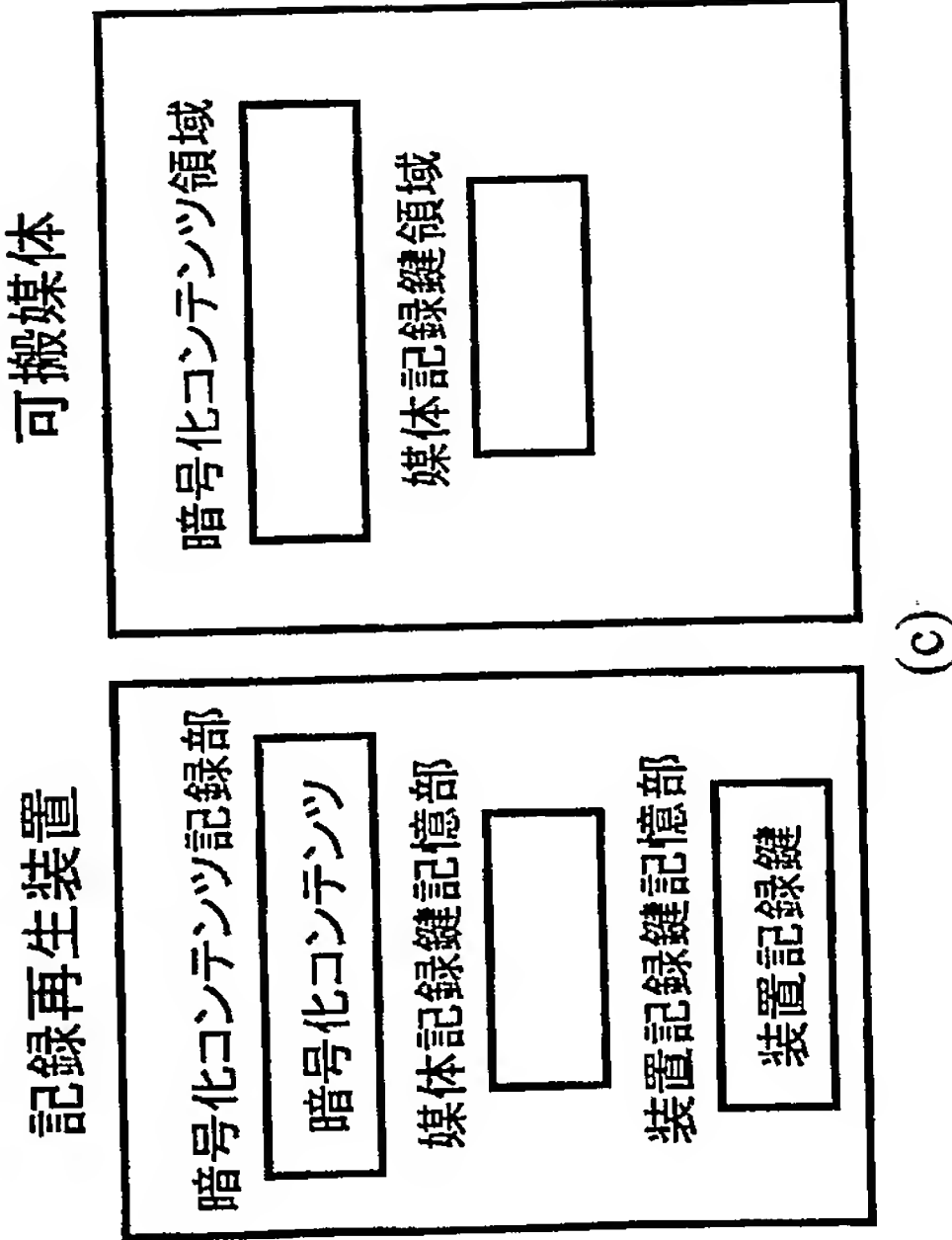
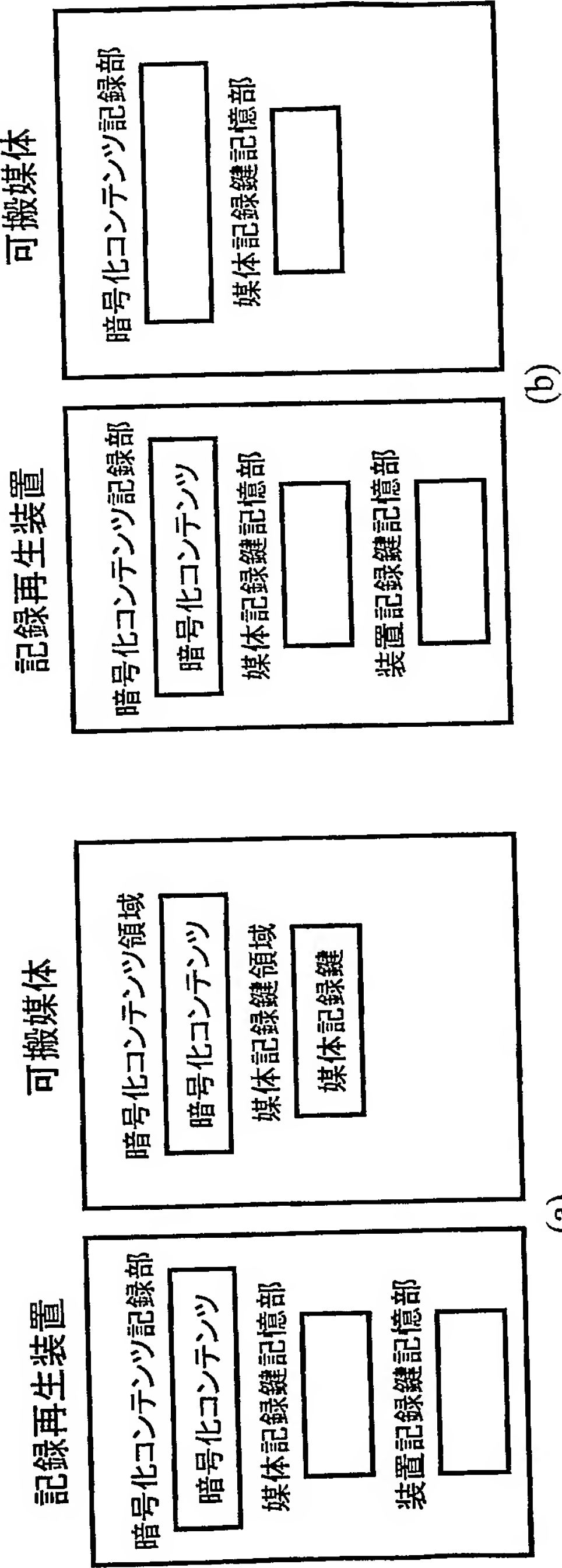
【図 14】



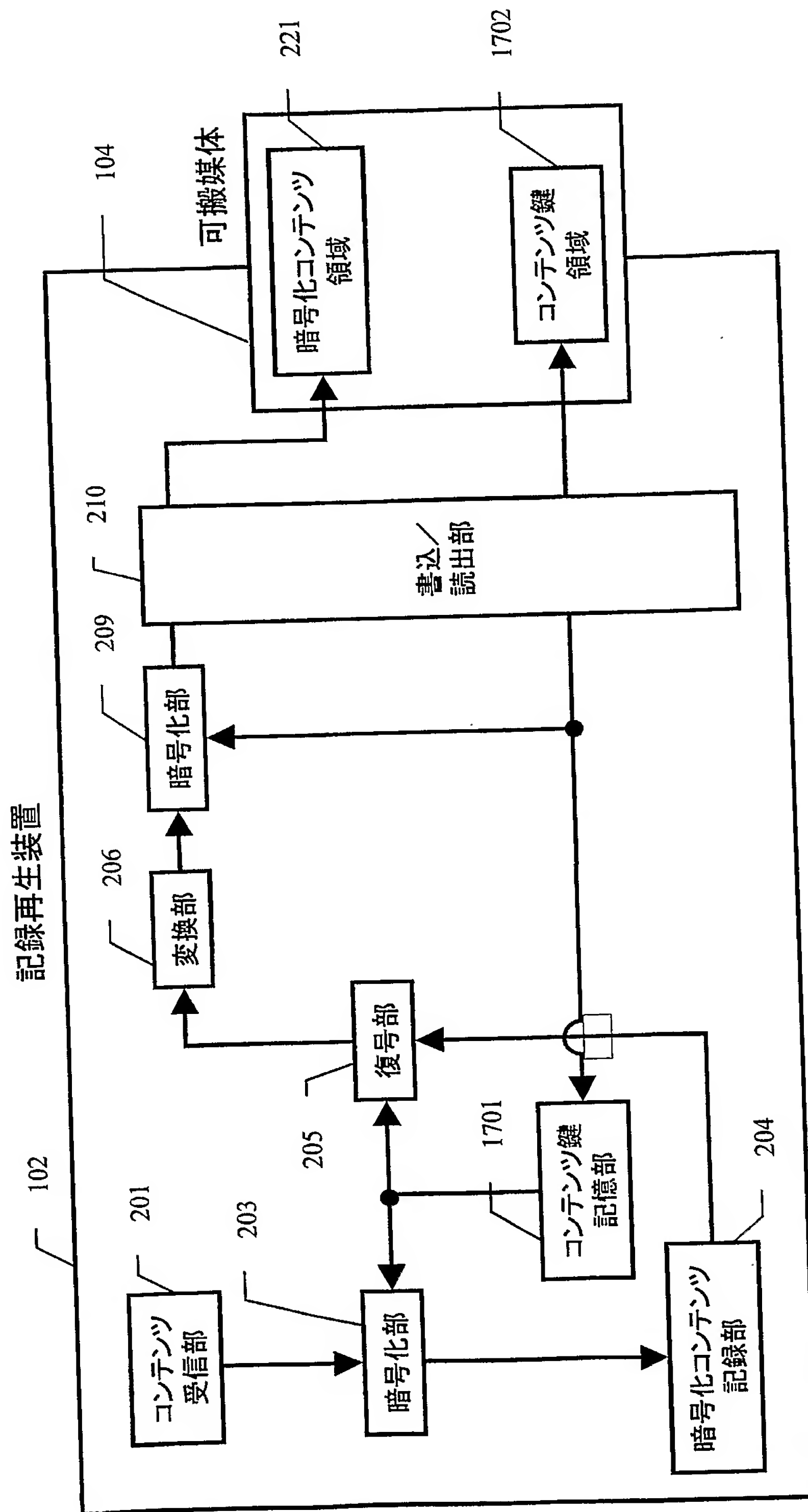
【図 15】



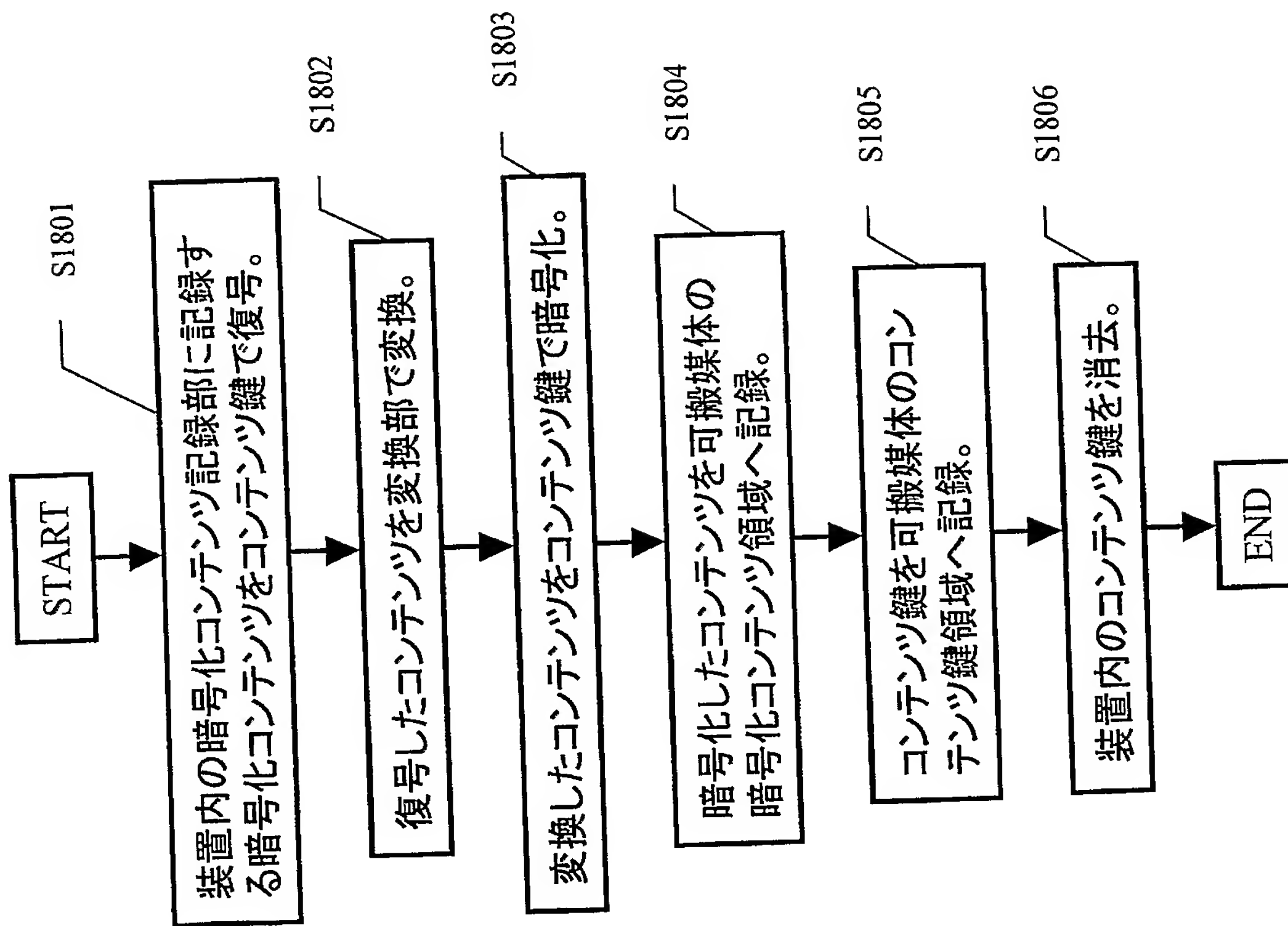
【図 1 6】



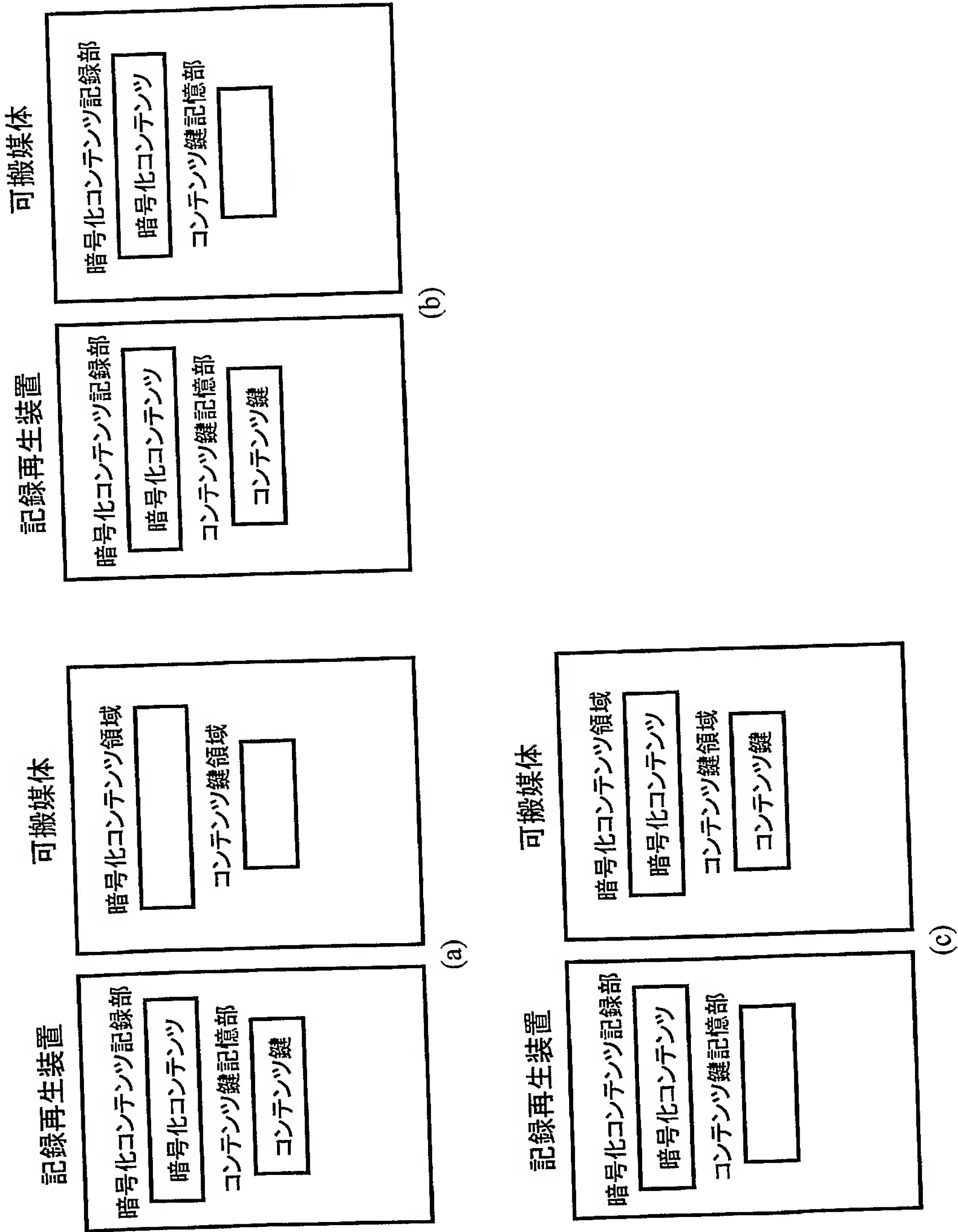
【図 17】



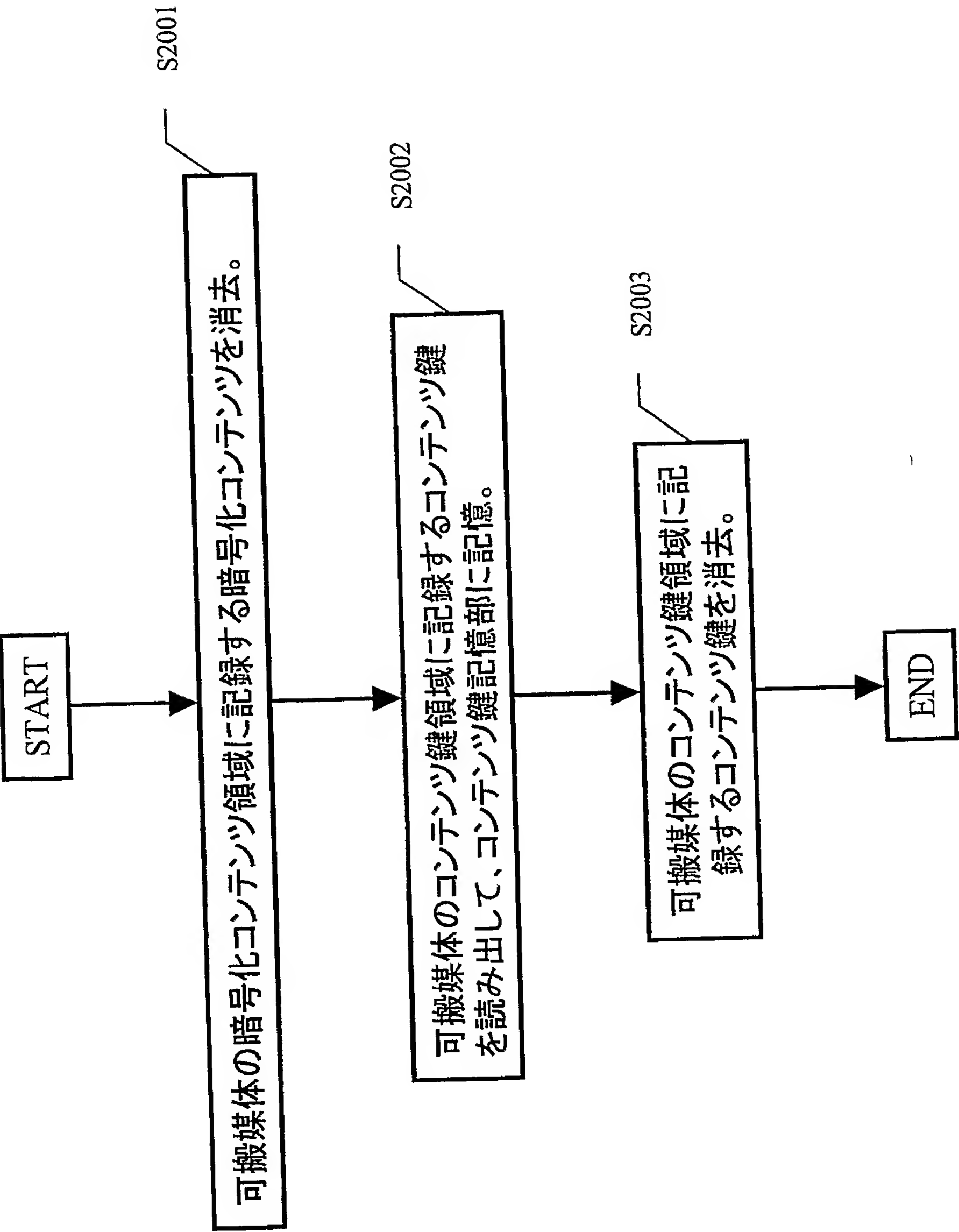
【図 18】



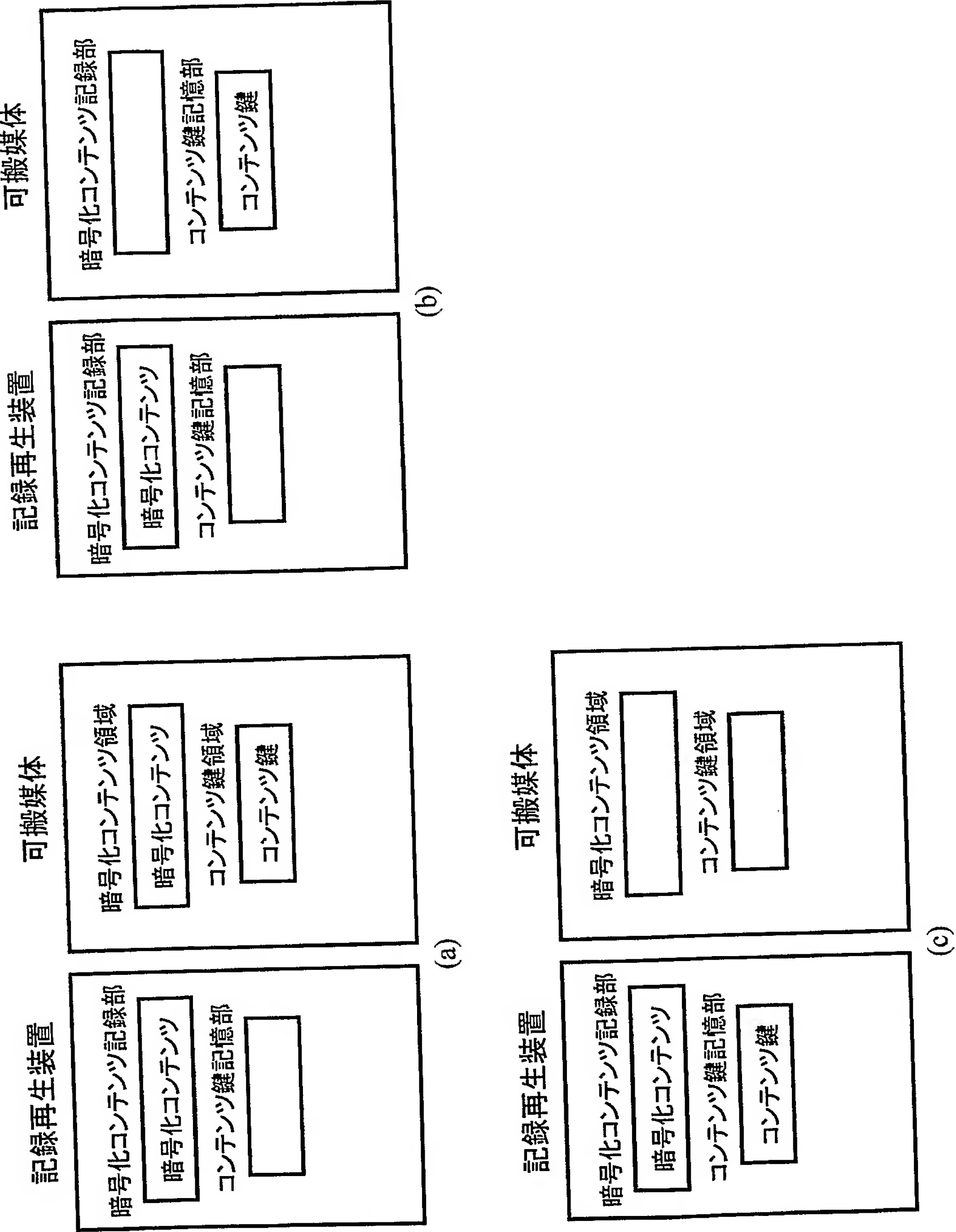
【図 1 9】



【図 2 0】



【図 2 1】



【書類名】 要約書**【要約】**

【課題】 移動元のコンテンツが高画質コンテンツであり、その画質を劣化させるなどしてサイズを小さく圧縮変換してからコンテンツの移動を行った場合、圧縮変換されたコンテンツだけがユーザの下に残り、高画質コンテンツが失われてしまう。

【解決手段】 コンテンツの移動時に当該コンテンツを復号するための鍵も合わせて移動させることにより、記録再生装置内のコンテンツを消去せずに利用不可状態にすることで、移動したコンテンツを再び戻す場合に、前記復号鍵を移動させることにより、元々の高画質コンテンツを利用可能にする。

【選択図】 図 1

特願 2 0 0 4 - 0 2 6 8 5 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社